DRONE, INC.

Marketing the Illusion of Precision Killing

FRONT COVER: TOP PHOTO: Newspaper collage by Brave New Films.
JOYSTICK: Pilot at Creech Air Force Base, Nevada. CREDIT: Christian Clausen, U.S. Air Force.

Table of Contents

PREFACE
Question the Numbers

Less than a fortnight after Donald Trump took office as president, the U.S. launched a major helicopter raid in Yemen, followed by a barrage of 70 drone-led air strikes over the course of five weeks.[1]

In the first three months of 2017, such drone attacks killed as many as 70 people, including an estimated dozen children and a three-month-old baby.[2]

The numbers are not different from previous years; nor are they less precise. Such numbers suggest that intelligence failures intrinsic to the drone war have routinely resulted in a serious toll of civilian casualties.

DRONE, Inc.: *Marketing the Illusion of Precision Killing* is the story of the unmanned aerial surveillance platforms used to plan many capture/kill military operations today. They employ **hardware** such as cameras and phone trackers, **software** for identifying targets; and **contractors** who supply and support the technology.

In July 2016, the Obama administration released a report claiming that drone strikes and related counterterrorism operations killed 2,581 individuals in countries where the U.S. is not officially at war. The White House admitted that between 64 and 116 of this number were innocent civilians.[3]

Yet the *Bureau of Investigative Journalism*, a U.K.-based nonprofit media organization which keeps a regular tally, estimates that as many as one in five drone victims has been a civilian.[4] Prominent human rights organizations like Amnesty International and Human Rights Watch have documented dozens of on-the-ground, examples of victims not included in the official U.S. figures.[5]

One internal Pentagon study showed that civilians were killed or wounded in 21 specific strikes in Afghanistan, despite the fact that in 19 of those 21 cases, preliminary evaluations conducted via drone cameras identified not even one civilian casualty.[6]

That's not all. "These 'high value targets' appear to be doing the impossible—dying not once, not twice, but as many as six times," said Jennifer Gibson, staff attorney at Reprieve, a U.K. human rights organization.[7]

How can there be such wide discrepancies between the official count and those of independent observers and insiders? The Obama administration's July report contains a clue:[8]

> *Government post-strike reviews involve the collection and analysis of multiple sources of intelligence before, during, and after a strike, including video observations, human sources and assets, signals intelligence, geospatial intelligence, accounts from local officials on the ground, and open source reporting.*

Drone, Inc. explains why those "*video observations, signals intelligence, geospatial intelligence*" make major mistakes. After analyzing Freedom of Information Act requests, locating previously unpublished court documents, reviewing dozens of engineering and technical studies, and crunching contract data, a different picture emerges: Planning for drone operations was handicapped by a fog of numbers and raw data derived from flawed technology marketed by contractors, the military and the intelligence agencies. Indeed, because of erroneous assumptions about these new technologies and a failure to properly evaluate ongoing operations, the U.S.—under Obama and now Trump—is conducting a deeply inaccurate remotely controlled war.

The Dawn of the Networked Drone

Drone technology is neither new nor uncommon any longer. Hobbyists now buy millions of camera-equipped quadracopters annually to film themselves from the air; commercial entities use drones are being used for all manner of activities from crop inspections to film-making.

Military drones—notably the Predator and Reaper—that are used for targeted killing, however, bear little resemblance to these consumer models. They are primarily surveillance platforms bristling with sensors that have become key nodes in the complex global networked system of intelligence gathering for the War on Terror.

Three experiments in 2001 illustrate the evolution of these networked military drones. The first experiment was an attempt to use a drone video camera to track down a target and then fire a missile at it. The second was an attempt to pinpoint the ground-based source of a radio signal and point a drone video camera at it. And the third experiment was to share all these video, radio and location data among observers in multiple locations in "real time," *i.e.,* as it was happening.

These incremental experiments took on a profound importance because of what happened next: The Sept. 11, 2001 attacks in New York and Washington DC galvanized the Pentagon to speed up development of these drone technologies to help the military wage war in places where it was either

politically or logistically difficult to deploy troops.

All three experiments had taken place in California, in many ways the birthplace of the military drone. General Atomics, the company that makes the Predator, the Reaper as well as Hellfire missiles, is based in San Diego. Some of the key military bases and testing ranges such as China Lake, El Mirage Airfield, Edwards Air Force Base and Camp Pendleton are also located in central and southern California.

Experimental drone being tested at El Mirage. CREDIT: Alan Waide, National Aeronautics and Space Administration.

MTS-A

The first experiment—using a drone to locate and fire on a remote target—was part of a scheme dreamed up by a secretive Air Force technology development program known informally as Big Safari. It took place on April 4, 2001, when William Casey of Raytheon joined Chris Dusseault of General Atomics at El Mirage Airfield. There, Raytheon's Multi Spectral Targeting System (MTS)—a makeshift test "ball" of electronic sensors—was attached to the bottom of a General Atomics Predator drone. [9]

Inside the 124-pound, 19-inch-tall grey metal ball was a video camera, an infrared camera, and a laser pointer (called a designator) that could help guide a missile. But the data that streamed back from the drone were not promising, according to Richard Whittle, author of the book *Predator*, who interviewed many of those present. "Tracker sucks!" one crew member complained. "Focus sucks!" said another, and a third added: "Color sucks!" Worst of all, the video camera and laser were misaligned, making it hard to confirm that the missile hit the intended target.

Predator sensor ball.
CREDIT: Cohen Young, U.S. Air Force.

Dragonfly

The second experiment tried to address the problem of finding targets. The MTS-A camera provided what drone operators call a "soda straw," or a view that is essentially restricted to a very narrow pipe, making it hard to follow multiple targets or scan the horizon. The video quality was also too poor to identify people on screen. If, however, other intelligence could be used to automatically point the camera at the desired target, then drones could be used to hunt, not just to fire missiles.

Dragonfly device.
CREDIT: Offered for sale on HelloTrade.

The Dragonfly—a radio tracking sensor manufactured by Ticom Geomatics, a start-up in Austin, Texas —was programmed to serve as part of a networked sensor system that could locate radios on the ground, allowing drone operators to target a specific radio device rather than having to find and identify targets using the video feed. The system would eventually become automated, directing camera operators towards targets with no human intervention. It was tested in June 2001 on aircraft at Camp Pendleton.[10]

Distributed Common Ground System

In the third experiment, also in June 2001, Army soldiers at the China Lake Base attempted to share data with a Navy control station on the U.S.S. Coronado, an experimental command ship off the California coast, near Camp Pendleton. The relatively new computer network that routed the data, the Distributed Common Ground System (DCGS), was maintained by Northrop Grumman of Virginia and Lockheed Martin of Maryland, among other contractors.[11]

"The Army and Navy demonstrated significant interoperable network centric capabilities," Maj. Jim Chapman told the *Eagle*, the Army Space and Missile Defense Command's magazine. "The experiment was [an] unqualified success." But, as will see, he was much too optimistic.

Ramping Up

Barely three months after the summer experiments, four planes crashed into targets on September 11, 2001, and soon after, the U.S. went to war in Afghanistan. Gen. John Jumper, commander of the Air Combat Command, ordered a ramp-up of the Big Safari drone program.[12] Before the contract was canceled in 2010, the Pentagon bought 268 Predator drones from General Atomics in San Diego. In 2007, when General Atomics released the more advanced Reaper drones, the Pentagon ordered 329 of the newer aircraft. [13]

This report will focus on sensors carried by the Predator and the Reaper, which are the principal aircraft used for targeted killing. We will, however, occasionally reference other drones such as the Global Hawk, as well as the piloted planes that complement and extend the targeted killing system (see box).

Piloted Surveillance Aircraft

Drones are essentially a modern version of the piloted U-2 aircraft that spied on the Soviet Union in the 1950s from a height of 60,000 feet. Those surveillance planes shot and brought back physical film that the Pentagon later developed and analyzed. [14]

Joint Surveillance Target Attack Radar System aircraft crew. CREDIT: Rey Ramon, U.S. Air Force.

Today, U-2s are still in service but their pilots now relay digital photos and electronic surveillance in real time via satellite links, just as drones do. In fact, since U2s don't have to relay video to pilots on the other side of the world, they can carry much more sophisticated sensors than the Predator or Reaper. [15]

The military also regularly uses other piloted but unarmed surveillance aircraft to gather data. Most are modified civilian aircraft like the Project Liberty program which uses retrofitted Beechcraft King Air 350s,[16] JSTARS (Joint Surveillance and Target Attack Radar System), [17] and Rivet Joint aircraft that use modified Boeing C-135s.[18] The latter aircraft carry up to 30 crew and can stay aloft for 8-10 hours. The U.S. also uses smaller aircraft like the Cessna and Pilatus.[19]

HARDWARE
Watching from Above

ANATOMY OF A DRONE

A military drone's surveillance sensor system is a sophisticated stand-in for a pilot's keen senses. Drone "eyes" include a suite of cameras that can transmit video and heat signatures, plus radar antennas that can map the precise

ANATOMY OF A DRONE

C-band antenna

GPS antenna

Radio & phone signal tracking equipment

Ku-band satellite communications antenna

Video & infrared sensor ball

Synthetic aperature radar (SAR) antenna

Hellfire missiles

1 - Video & Infrared

2 - Radar Imaging

3 - Signal Tracking

dimensions of large objects and ground terrain. The "ears" include receivers to detect and collect radio frequency signals from mobile phones and tactical radios within range. Finally the "head," located on top of the drone, carries a GPS device and an "inertial navigation system" to calculate the drone's location and a directional satellite antenna to track and transmit its catch to relay satellites that route the data around the world for analysis and targeting.

Most of these sensors are housed under the nose of the aircraft in a ball that holds two video cameras (one with a zoom lens), an infrared camera, and a laser system to pinpoint (aka "paint" or "sparkle") targets. In addition, drones can carry a separate 3-D imaging system and a radar system.

Drones are organized into "combat air patrols" of three to four aircraft, each with a pilot and sensor operator. But a full crew can consist of as many as 180 individuals, including radio technicians, safety observers, video analysts, still imagery analysts, and strike coordinators and commanders. In addition, support crews launch, recover, maintain, and refuel the drones at local airfields close to the action. [20]

The U.S. currently fields about 60 such patrols around the world at any given time. Despite White House pressure to increase the number to 90, a severe shortage of trained pilots has impeded a quick expansion. [21]

Human Activity
Predator vs HDTV – 3 mile slant range

HDTV, 1200 mm focal length

Predator, 955 mm focal length

UNCLASSIFIED

A. Full Motion Video

The two most important, and quite different, functions of military drones are keeping watch over troops and identifying potential enemies. While troops can and want to identify themselves to drone personnel, hostile forces do their best to camouflage their movements and blend into the background and civilian populations.

Imagery analysts, who act as guardian angels to fellow soldiers under attack, report immense job satisfaction. "It's not just blips on the screen and video games," Amy, a National Guard civilian who works in drone surveillance at Joint Base Langley-Eustis, told the *Virginian Pilot* newspaper during a March 2015 day tour for the local media. "These are real people, and they have families and lives and, in that moment, you are the person ... that is making sure they are protected."[22]

Their role is especially gratifying in times of conflict. "If there is an op going on, the guys on the ground can't see over a wall, they can't see on the other side of a building or a hedgerow," Caleb, an Air Force lieutenant told the same newspaper. "We can say, 'Hey, you got three dudes on the other side of this wall right over here, so watch for them'... or 'We just saw a child come out of this building, there's a woman there, we can't strike this. Call off the strike right now.'"

Yet even on these occasions, the cameras that military drones carry are surprisingly limited. In April 2011, a Predator was assigned to support Marines involved in a ground battle with the Taliban in Afghanistan. The commanders made a judgment call

"We can see Border Patrol, but not their uniforms. [If] we can communicate with them and say, 'Wave your arms' …we can distinguish between our guys and the bad guys,"

—Lothar Eckardt, National Air Security Operations Center in Corpus Christi, Texas

based on muzzle flashes and called in a Hellfire missile strike, only to discover that they had targeted and killed Jeremy Smith and Benjamin Rast, two U.S. soldiers in full battle uniform.[23]

Later Jerry Smith, Jeremy's father, was shown video of the strike. All he could see, he told the *Los Angeles Times*, was "three blobs in really dark shadows. You couldn't even tell they were human beings—just blobs." It was impossible, he noted, to identify their uniforms or weapons or differentiate U.S. soldiers from Afghans.

Indeed, Predator operators on the U.S.-Mexico border say they have to rely on direct radio contact to overcome similar limitations. "We can see Border Patrol, but not their uniforms, and so we can communicate with them and say, 'Wave your arms,' and that way we can distinguish between our guys and the bad guys," Lothar Eckardt, director of the Department of Homeland Security's National Air Security Operations Center

in Corpus Christi, Texas, told the *Washington Post*.[24]

Drones are often touted as able to read a license plate from two miles away, but operators say this is rarely true. "The video provided by a drone is not usually clear enough to detect someone carrying a weapon, even on a crystal-clear day with limited cloud and perfect light," Heather Linebaugh, a former Air Force imagery analyst, wrote in the *Guardian* newspaper in 2013.[25]

"This makes it incredibly difficult for the best analysts to identify if someone has weapons for sure. One example comes to mind: The feed is so pixelated, what if it's a shovel, and not a weapon?"

Usually, the best an analyst can hope for is to follow one group of people, and distinguish men from women or adults from children, but even that can be difficult, as the Uruzgan example (see box) shows. In Central Asia and the Middle East where most men wear very similar clothes and have the same color hair and skin,[26] identifying an individual from a Predator at 10,000 feet is essentially impossible. Facial recognition is also impossible without a camera located at eye level.[27]

Using video for observation has also been found to increase human error. A Grumman Aerospace study conducted by Pierre Sprey in the 1960s, found that observers watching aerial video tend to identify as many as five times more false objects as observers watching with the naked eye.[28]

So what cameras do Predators and Reapers carry, and why don't they provide better imagery?

The Cameras

The system of choice for over a decade has been Raytheon's MTS-A ball, which has two video cameras installed as part of the standard package. One is a color camera mounted on the nose to help the pilot steer; the second is a RS-170 Versatron camera for looking down at subjects.[29]

The Versatron transmits pre-digital TV-standard quality: 512x480 pixel images. It is good enough when filming close up, but from a height of 10,000 feet, even with image intensification technology, the average person is reduced to a splotch. Since the camera has a 16-160mm zoom lens as well as a 955mm spotter lens, a camera operator can zoom in and read to the detail of a license plate, but not much else at the same time, because of the "soda straw "restriction of the field of view. For most of the last 20 years, these older cameras were standard.[30] The Air Force has now mostly replaced the Raytheon MTS-A ball with the more advanced MTS-B or the heavier Wescam MX series made by

L-3 Communications of New York, which carries a high definition camera and is used on piloted surveillance aircraft. [31]

Video Quality

The quality of a full-motion video camera's imagery can be determined by the Video-NIIRS rating (V-NIIRS) of the feed. The standard is based on the National Imagery Interpretability Rating Scale (NIIRS) which assesses the clarity of still photography.[32]

With a V-NIIRS rating of 5, the Versatron cameras on the original MTS-A sensor carried by the first Predators could watch over troops in a vehicle, but definitely not identify them, even by their uniforms.

An image with a V-NIIRS rating of 6 has the potential to find an individual who is isolated, but not one in a crowd. A V-NIIRS-7 allows an observer to track an individual wandering through a crowded market; V-NIIRS-7.5 can capture simple hand movements like picking up a mobile phone. V-NIIRS-8 is required to positively identify a man from a woman or child. An image rated at V-NIIRS-8.5 is needed to track a person firing an assault rifle, but still would not be able to identify someone using a small pistol.

CREDIT: Institute for Defense Analyses.
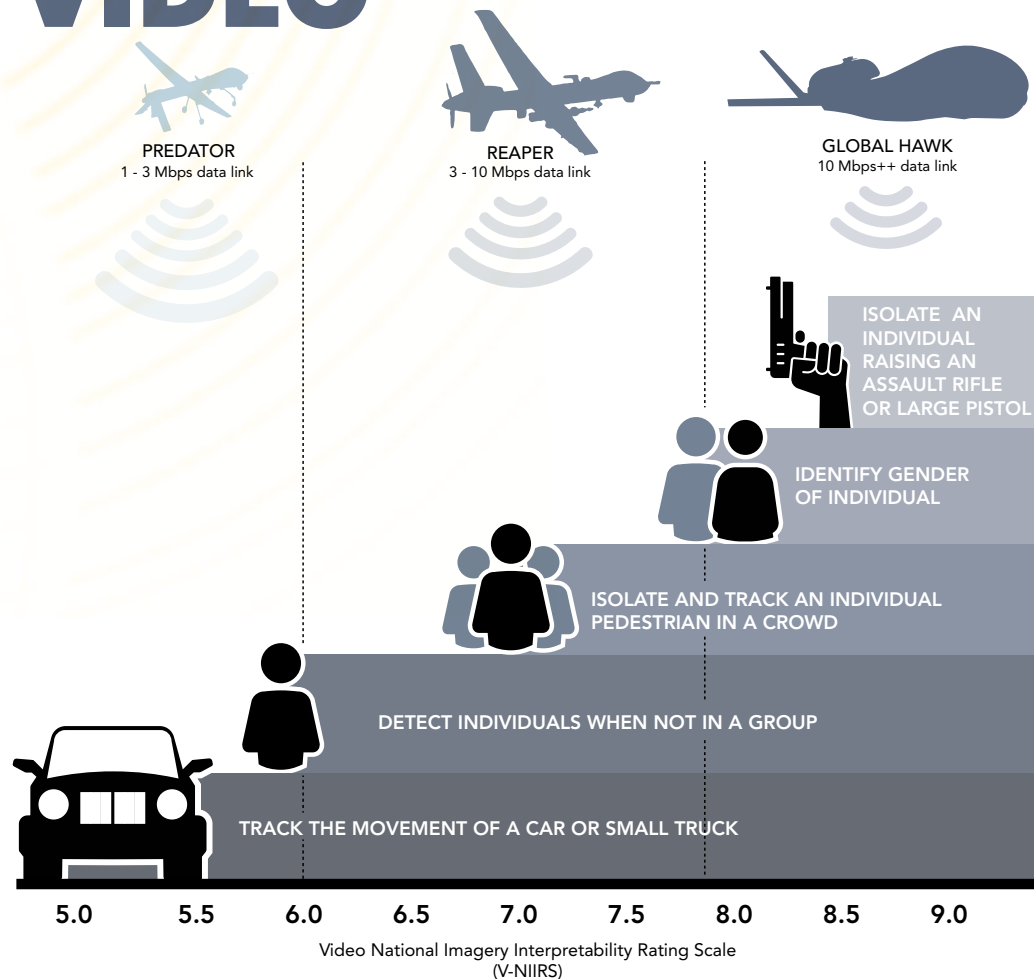

NIIRS 4 (≈ 6' GSD)   NIIRS 6 (≈ 2' GSD)   NIIRS 8 (≈ 6" GSD)

VIDEO

PREDATOR
1 - 3 Mbps data link

REAPER
3 - 10 Mbps data link

GLOBAL HAWK
10 Mbps++ data link

ISOLATE AN INDIVIDUAL RAISING AN ASSAULT RIFLE OR LARGE PISTOL

IDENTIFY GENDER OF INDIVIDUAL

ISOLATE AND TRACK AN INDIVIDUAL PEDESTRIAN IN A CROWD

DETECT INDIVIDUALS WHEN NOT IN A GROUP

TRACK THE MOVEMENT OF A CAR OR SMALL TRUCK

5.0 5.5 6.0 6.5 7.0 7.5 8.0 8.5 9.0

Video National Imagery Interpretability Rating Scale
(V-NIIRS)

These numbers explain why imagery analysts see individuals as "blobs." Notably only the MX-20 or MTS-B ball, carried by newer Reapers and piloted surveillance aircraft, approach the quality to identify men from women. [33]

One of the major reasons that drones carry such low resolution video cameras is the limit in the amount of data a drone can transmit in real time to overhead satellites. Predators initially fielded modems that broadcast at 1-3 megabits per second (Mbps), and Reapers no more than 10 Mbps. (see "Relaying the Data "section). Even using the Reaper's high

rate, an imagery analyst cannot identify a person's distinguishing facial features.

Location Data

While most discussions of drone footage tend to focus on quality and detail, those are not the only critical factors. Archival video, which analysts need to determine patterns of life (especially since the operators work in shifts), needs to have precise location data. To that end, drones transmit a code alongside the image. For analog video this is encoded on Line 21 of the signal (the same as closed captioning), while digital video carries a

KLV (Key-Length-Value) code. Since the analysts need to be able to compare video footage, the Line 21 code from analog video is supposed to be converted into KLV codes at a ground station. But this transformation often fails.[34]

What that means, in plain English, is that location details for older Predator video feeds often have been lost. Recently, the Defense Information Systems Agency (DISA) became concerned that the video metadata was often discovered to have "incorrect values, missing keys, and corrupted data."

To determine the prevalence of this problem, DISA conducted an experiment to archive and study a week's worth of data from 80 surveillance aircraft, many of which were drones, operated by the Pentagon in mid-March 2013. [35]

The results showed that only two out of three aircraft were able to provide location data. In addition, the quality of their data varied wildly: Predators and Reapers using analog video only provided complete data once every 2-4 seconds, or roughly one percent of location data transmitted by the more advanced piloted reconnaissance aircraft, which recorded their location 30 times a second.

There is another problem with location data from drones—a phenomenon known as "inherent error" that stems from a variety of factors such as drift and ionospheric effects. These can cause measurements to be inaccurate by as much as 20 meters, unless the system is calibrated and controlled by a skilled operator.[36]

While the use of landmarks and imagery databases can often help correct these machine errors, the system is by no means perfect. "Imagery analysis is time and resource intensive. Rectification, georectification, and orthorectification operations must be performed by a trained specialist on unique equipment with purposeful access to updated reference imagery databases," writes Marine Capt. Patrick Coffman in his 2015 thesis for a master's degree in Information Warfare Systems Engineering. "If any of these components is missing, the procedure cannot be completed."

Coffman described a Marine Special Forces operation in western Afghanistan where 30 analysts had to be brought in to accurately identify a single target in a two-block urban environment. "Why is it so difficult to exploit motion imagery derived from UAVs?" he asked rhetorically in his thesis. "Why does it take special equipment and training to do what Google Earth can in my living room? In the most technologically advanced military this world has seen, this operational restriction is nearly laughable, if not utterly frustrating."[37]

Of course, the video camera is only one of the sensors on a drone. Far more important are the devices used to "geolocate" mobile phones. We'll get to that after we discuss the other visual sensors available to drone analysts: infrared technology, thermal imagery and radar tracking systems.

Drone Strike Kills 23 after Video Feed Fails to Identify Women and Children

A convoy of three vehicles was winding its way through the empty back roads of rural Uruzgan Province, Afghanistan, early on a Sunday morning in February 2010, when U.S. forces fired a series of missiles at it. Between 15 and 23 people were killed, including two boys under the age of five. [38]

An exhaustive investigation led by Maj. Gen. Timothy McHale, who interviewed more than 50 witnesses, later established that not one of the victims was an "insurgent" or a "terrorist." All were villagers, just going about their business. [39]

A drone crew, based at the Creech Air Force Base in Nevada, which had been tasked with protecting a foot patrol of U.S. soldiers in the area, was blamed for the mistake. Excerpts from a transcript of the conversations between Creech operators, video analysts at Air Force Special Operations headquarters in Okaloosa, Florida, and an overhead helicopter crew in Afghanistan, revealed the series of errors that led to the strike.
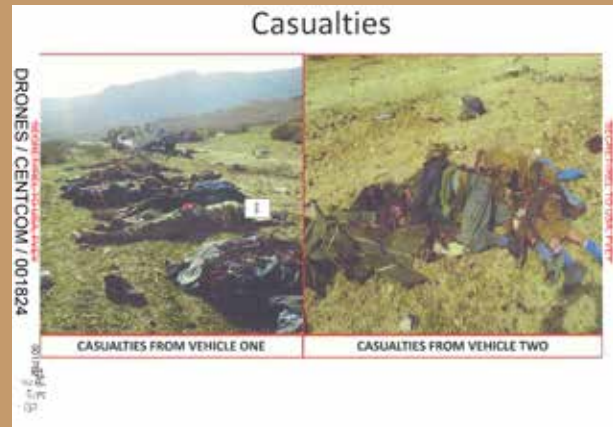
"The [military-aged male] that just mounted the back of the [Toyota] Hilux had a possible weapon, read back possible rifle."

"Be advised there was a brief scuffle, looks to be potential use of human shields, but definite suspicious movement, and definite tactical movement."

"Be advised, our screener just called one [military aged male] near the SUV, appears to be holding a weapon."

"Our screener just called out one additional weapon. Was laying on the ground, where praying, picked it up and now has entered the truck."

About 20 minutes after the missiles had been fired, the chat transcript reveals that the soldiers realized that not only was the video feed too pixelated for them to identify women and children, the weapons call was also wrong.

Casualties

CASUALTIES FROM VEHICLE ONE | CASUALTIES FROM VEHICLE TWO

DRONES / CENTCOM / 001824

Aftermath of Uruzgan strike. CREDIT: U.S. Central Command investigators.

"The thing is, nobody ran."

"Yeah, that was weird."

"Uh, have you been able to positively identify any individuals with weapons at this point?"

"Yeah, there's definitely no weapons on the guys in the middle vehicle."

"Let's keep looking at whatever."

"We looked at all of them and I don't think that any of them have weapons."

"They're trying to surrender, I think."

"I personally wouldn't be comfortable shooting at these people."

"Believe possibly two of those, maybe 3, were female. They wore bright colored clothing."

"He's calling females? They said 21 males, no females."

"Dude, we watched these guys stop multiple times and every time they were all wearing all black and only afterwards did we ever see any color."

"It's possible the…the women and children never got out of the car, at the stops."

"Be advised we do have what looks to be 3 women and 2 children possibly trying to surrender."

B. Thermal & Infra Red Imaging

On January 15, 2015, two U.S. missiles struck a house in Shawal, North Waziristan, setting it on fire and killing everyone inside. The drone crews on the other side of the world had been told to expect four victims. To their astonishment, they watched as six bodies were pulled from the wreckage and given Muslim burials.[40]

A little over three months later, a grim faced President Obama announced: "One American, Dr. Warren Weinstein, and an Italian, Giovanni Lo Porto ... were tragically killed in a U.S. counter-terrorism operation. …Based on the intelligence that we had obtained at the time, including hundreds of hours of surveillance, we believed that this was an al Qaeda compound; that no civilians were present."[41]

Obama's official statement leaves no doubt that the U.S. intended to bomb the compound and kill all those inside the building. Intelligence officials later said that the more than 400 hours of video compiled over several weeks had determined only four individuals were present, all of whom they believed were militants.[42]

To comply with 2013 rules requiring "near-certainty" that no civilians were targeted, the analysts had taken another measure. "To make sure nobody else was hiding inside the compound, the CIA used the drone's heat sensors, which

LEFT: Warren Weinstein.
CREDIT: Weinstein family.
RIGHT: Giovanni Lo Porto.
CREDIT: Lo Porto family.

can detect the unique heat signature of a human body," Adam Entous reported later in the *Wall Street Journal*. [43]

What is striking about this admission is that neither the video cameras nor the heat sensor had revealed the presence of two additional adult men living on the premises.

> ## "Aerial infrared imagery turns all bodies into indistinct human morphologies that cannot be differentiated according to conventional visible light indicators of gender, race, or class."
>
> **—Lisa Parks, University of California Santa Barbara**

It's not altogether surprising that that video imagery was poor but what is more problematic is that the back-up heat sensor also failed.

The Predator and Reaper use forward-looking infrared sensors (FLIR) that come as standard on both the MTS and the L-3's Wescam MX series sensor balls.[44] Other drones often use an infrared

Drone infrared imagery.
CREDIT: Ministry of Defence, UK.

imager made by Oregon-based FLIR Systems. [45]

FLIR cameras have an advantage over radar because they do not send out pulses that might be detected by a target, while still seeing through smoke, haze, and light fog. Drone operators often use them at night, but even during the day heat signatures are supposed to be able to help analysts detect heat sources such as warm bodies and weapons. However, image quality is limited by humidity, pollution, rain, and distance from the target. (Short-wave infrared cameras are available for low light situations and long-wave infrared cameras are available to penetrate smoke, dust, and clouds, but using both at the same time can be impractical and expensive.)[46]

There are other problems with FLIR heat sensors. They cannot distinguish one person from the next, cannot see through trees and can be fairly easily thrown off by hot days, the profusion of heat sources in urban areas, and even by a well-placed blanket that dissipates body heat. Nor can they see into base-ments or underground bunkers.

It is also hard to distinguish one inani-mate heat source from another, partic-ularly when filming from 10,000 feet and above. Lt. Col. Mark McCurley, a former Air Force drone pilot, who is an unabashed supporter of Predators, reported that a junior analyst he worked with confused a cigarette with the muzzle flash of a gun. "On the infrared screen, smokers at night often looked

as if they held a miniature sun in their hand," McCurley wrote.[47]

Experts say that thermal imaging can actually reduce the accuracy of targeting because it can lead observers jump to conclusions. "Seeing according to temperature turns everyone into a potential suspect or target," writes Lisa Parks, director of the Center for Information Technology and Society at the University of California Santa Barbara. "While other systems of human differentiation and observation are organized around skin color, personal data, and/or facial recognition, aerial infrared imagery turns all

bodies into indistinct human morphologies that cannot be differentiated according to conventional visible light indicators of gender, race, or class."[48]

But on a winter night in the rural north of Pakistan, the heat sensors should have been operating under optimal conditions. Nonetheless, they were unable to identify the presence of Lo Porto or Weinstein in Waziristan. Likewise the erroneous killing of Jeremy Smith and Benjamin Rast in Afghanistan was based on the evaluations of heat signatures associated with weapons fire.[49] (see previous section)

Excerpt from conversation between drone personnel watching villagers in Uruzgan, February 2010 [50]

00:45 (Pilot): *What did he just leave there?*

00:45 (Pilot): *Is that a *expletive* rifle?*

00:45 (Sensor): *Maybe just a warm spot from where he was sitting; can't really tell right now, but it does look like an object*

00:45 (Pilot): *I was hoping we could make a rifle out, never mind*

00:45 (Sensor): *The only way I've ever been able to see a rifle is if they move them around, when their holding them, with muzzle flashes out or slinging them across their shoulders*
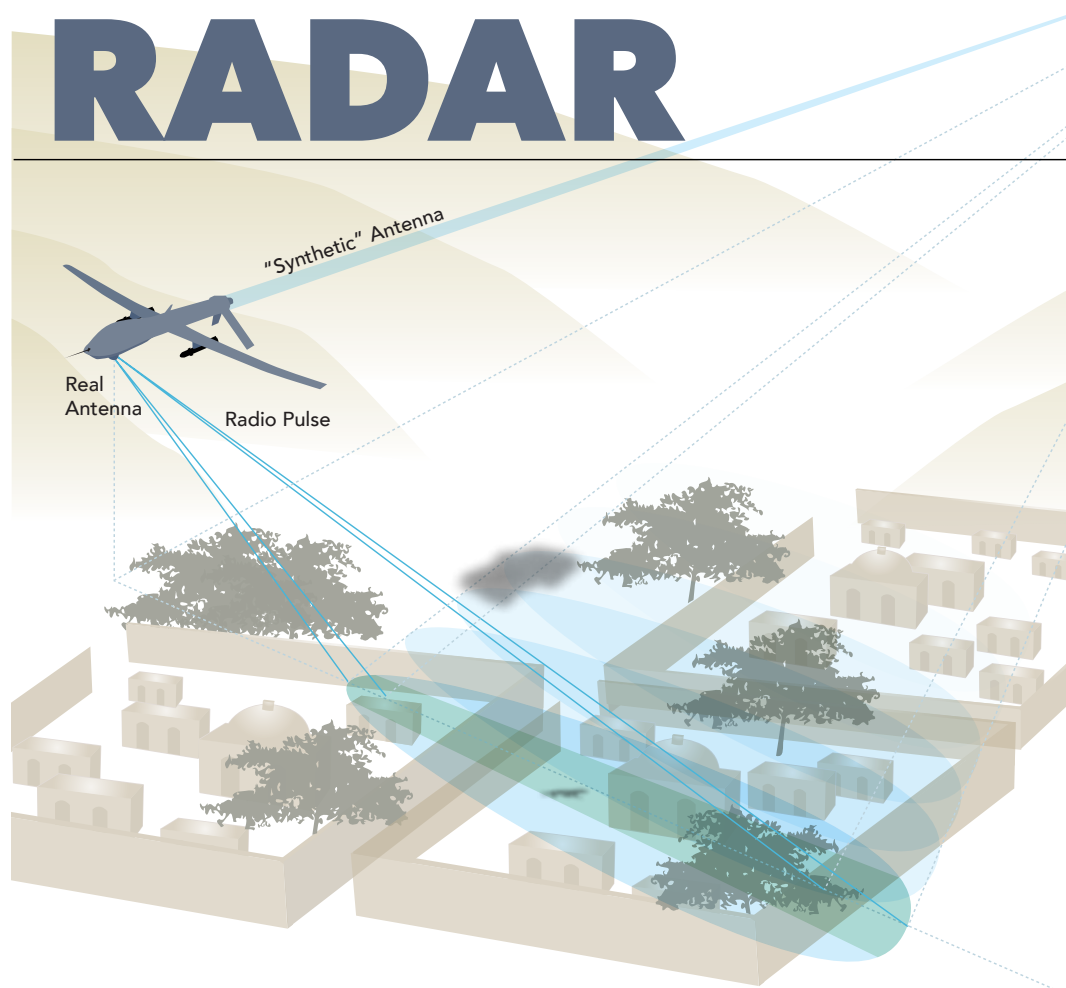
C. Synthetic Aperture Radar

In late August 1999, Sen. Pete Domenici joined Neal Blue, the CEO of General Atomics and C. Paul Robinson, the director of Lockheed Martin-operated Sandia Laboratories, at a ceremony in Albuquerque, New Mexico. They were there to unveil the Lynx, a 115-pound bright red gadget and to proclaim it the future of aerial observation.[51]

To this day, a version of the Lynx is still mounted on some Predators and Reapers. It uses "synthetic aperture radar," a technology invented in the 1950s, that fires multiple radar beams from a moving aircraft and then captures the bounce-back to create a three dimensional image. Unlike a camera lens that is pointed straight down, SAR's sideway-angled view can monitor a wider swathe of land. If an aircraft takes multiple pictures as it moves in a straight line, computers can then stitch together a panoramic picture of the terrain below.[52] Another system, Tactical Endurance Synthetic Aperture Radar (TESAR), manufactured by Northrop Grumman, is also available as an option for the Predator.[53]

SAR offered the advantage of being unaffected by most bad weather. "Cameras provided good data, but they don't work at night or in rainy, foggy and cloudy situations," Bill Hensley, the Sandia project leader, said at the New Mexico unveiling. "Fine-resolution image SAR radar is perfect for these circumstances because it can 'see' in the dark and peer through clouds and fog."

Lynx synthetic-aperture radar being installed on a drone. CREDIT: Randy Montoya, Sandia Laboratories.

RADAR

"Synthetic" Antenna

Real Antenna

Radio Pulse

The image SAR produces looks like a clay model of terrain. It can capture objects as small as four inches in diameter over areas as wide as tens of miles. What excites the military most about modern SAR imaging is an add-on technology called "coherent change detection" that allows a computer to compare images from multiple missions and alert users to movements or changes, such as vehicles or even a walking person. [54]

"An IMU is a collection of instruments that make six independent measurements. There are at least twelve independent unknown errors that need to be corrected by an aiding scheme. Unless each error is made observable and identi able, ambiguity exists for all others."

The most sophisticated SAR system, carried by the F-35 jet fighter, is reputed to be able to zoom in and out of a landscape on command, but is far too heavy for drones. [55] Even the lightweight Lynx takes up a tenth of the Predator's weight.

Despite those advantages, SAR suffers from several problems. First is the Lévy

flight error, colloquially described as the "drunkard's walk." A target that moves randomly and quickly in many directions creates a smear across the image. [56] A soccer game or a market would render the images unusable. For this reason, coherent change detection has a very hard time tracking many small moving objects that exist in most natural environments.

The second major problem lies with the relationship between the SAR antenna and the "inertial measurement unit" (IMU) that is supposed to calculate the drone's position. Since SAR works sideways, when operators move the camera to improve video observation, the angle of the radar changes.

"If knowledge of radar's relative position were exact, then the image could be formed with perfect focus, ignoring atmospheric effects," Armin Doerry, the Sandia engineer who was one of the main developers of the Lynx, wrote in a January 2015 technical paper on SARs. "An IMU is a collection of instruments that make six independent measurements. There are at least twelve independent unknown

errors that need to be corrected by an aiding scheme. Unless each error is made observable and identifiable, ambiguity exists for all others." [57]
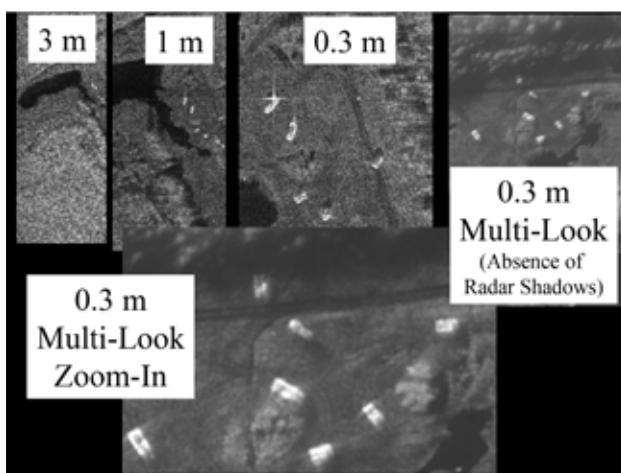
Doerry notes that GPS location does not help much in this matter since it only updates once a second and cannot provide the angle of the radar. To correct for this, an enormous amount of computing power is needed to calculate mapping in real time, or there must be many passes over an object— which defeats the idea of real-time observation.

SAR encounters another problem: scattering. In built-up urban areas or among the mountain slopes that it is required to map in countries like Afghanistan, the radar bounces back at unpredictable angles, depending on the location of the drone.

"Areas behind buildings lie in the radar shadows, and images of tall buildings can obscure other features of interest," wrote Margaret Cheney in a 2009 paper for the Naval Postgraduate School. "There is an added difficulty that that same object will look different when viewed from different directions." [58]

But it is not that SAR is imprecise or unusable. It can guide missiles and observe fixed locations to detect equipment being moved on or off a base or compound. And where it excels in the public interest is in mapping locations when an aircraft can repeatedly move in a specific direction at a specific speed. This function has enormous potential for scientific observations, from mapping the Moon to observing terrestrial glacial ice formations and landslides.[59] Unfortunately for tracking moving people, SAR remains a secondary and relatively useless sensor.

LYNX SAR

Under Secretary of Defense for Acquisition, Technology, and Logistics presentation. CREDIT: Dyke Weatherington.

Convoy Search Ft Dix: 2 x Cargo Trucks / 6 x Hummers

D. Phone Tracking

Nearly all mobile communication devices are designed to be tracked. A cell phone carrier, for instance, must generally know where all phones and towers in its network are at any given time. Otherwise a call placed in Karachi couldn't be directed through the network to its receiving phone in Paris.

The military understands and exploits this. It knows that mobile phones send signals every few seconds looking for nearby towers so they can be reached. Every time a cell phone pings a tower, the tower creates a record of that connection and tells the rest of the network. Thus intelligence agencies monitoring the network infrastructure, or receiving information from the service provider, can use this information to track phones as they transit tower coverage zones, known as "cells," around the world.

Even with access to that information, though, it is still a surprisingly difficult task to find the exact location of a cell phone. Cells can extend for miles and, contrary to popular belief, connecting to a given tower is not always an indication that a phone is within that cell.

Despite this, U.S. police routinely use mobile phone records to justify arrests. "Prosecutors often present those records as if they were DNA," Douglas Starr, the co-director of the graduate program in science journalism at Boston University, wrote in the *New Yorker* magazine. "Designed for business and not tracking, call-detail records provide the kind

of information that helps cell companies manage their networks, not track phones.[60]

Although it seems logical that a mobile phone would automatically connect to the closest tower, that's not always the case. Instead it sends a radio message to all the local towers it can find. At a regional switching center, special software routes a call by checking a host of factors: the phone's signal strength, the local weather, and what towers are shut for maintenance. Each mobile phone tower maintains a visitor location register, but there's no guarantee that the phone was actually close to it.

"Your phone wants the clearest tower," Michael Cherry, a former Bell Labs and NASA consultant who testifies on the science of cell-tower data in U.S. courts, said in an interview.[61] "But the clearest tower might not be the nearest tower, or even the tenth-nearest tower."

"The system is so fluid that you could sit at your desk, make five successive cell calls and connect to five different towers," adds Starr. "The switching center may look for all sorts of factors, most of which are proprietary to the company's software. The only thing that you can say with confidence is that I have connected to a cell site somewhere within a radius of roughly twenty miles." That's a little like knowing which county a house is located in but not knowing which town, let alone the street address.

In order to track mobile phones, the military uses radio locating devices known as IMSI catchers together with specialized software to conduct "geolocation," *i.e.,* the capability to locate a phone on a map. We'll discuss IMSI catchers first and then address geolocation software in a later section.

IMSI Catchers

An IMSI (international mobile subscriber identity) catcher works by the simple expedient of pretending to be a mobile phone tower and inviting all phones in the area to connect with it. Hackers have designed basic IMSI catchers for under $100. [62]

While the fake tower can easily get a list of all the mobile phones in range, it can only approximate, based on signal strength, how far away each connected phone is. If the IMSI catcher also has a "direction finding" antenna, it may be able to guess the rough direction that a signal came from. Mountains, buildings, and other objects can further degrade reception.

In theory, a strong signal from at least three different phone towers can allow a phone to be located. But even then, reverse-engineering a user's location from signal strength, direction and geography requires complex mathematical equations and computer algorithms.[63]

These techniques are extremely sensitive to measurement errors. In fact, the U.S. emergency phone system's mobile tracking accuracy rates are sometimes as low as 10 percent.[64]

Military drones also map local wireless access points such as WiFi routers to help further track targets. A document revealed by National Security Agency (NSA) whistleblower Edward Snowden gives one example of NSA attempts to map such devices in Oman in March 2012: "Flights and targets were coordinated with both CIAers and NSAers. The mission lasted 6 months, during which 43 flights were flown," an NSA staffer wrote about a mission code named Victorydance. "It was truly a joint interagency effort between CIA and NSA."[65]

But, as security experts note, this mapping is not an exact science since routers get moved, weather patterns disrupt signals, and phone towers have to be fixed. "If Google or Facebook get a physical location wrong, they show someone an ad for a restaurant they're nowhere near," Bruce Schneier, a security researcher, writes in *The Atlantic* magazine. "If the NSA gets a physical location wrong, they call a drone strike on innocent people." [66]

Indeed, no less an authority than the Federal Bureau of Investigation (FBI) warns its agents to be careful of relying on mobile phone trackers. "Using the results as evidence is generally discouraged because of the level of technical expertise required to effectively operate the equipment," an internal agency manual obtained by *The Intercept* states. "Accordingly, FBI employees should corroborate and verify the information obtained through other means."[67]

Prices and technical details of many of such devices were listed in a leaked "secret surveillance catalogue" recently published by *The Intercept.* Two IMSI catcher gadgets used on Predators or Reapers are the Airhandler and Gilgamesh, both made by the Nevada-based Sierra Nevada Corporation. Gilgamesh forces mobile phones within range to connect with it. Airhandler, meanwhile, serves as the antenna system for Gilgamesh, while also capturing signals from push-to-talk radios in the process. Both upload data to NSANet, a parallel Internet system managed by the NSA.[68]

PHONE LOCATION

The signal transmitted by a radio or a cell phone can be picked up by an IMSI catcher in a vehicle.

If the signal is picked up from two or more locations, the rough position of the phone can be calculated.
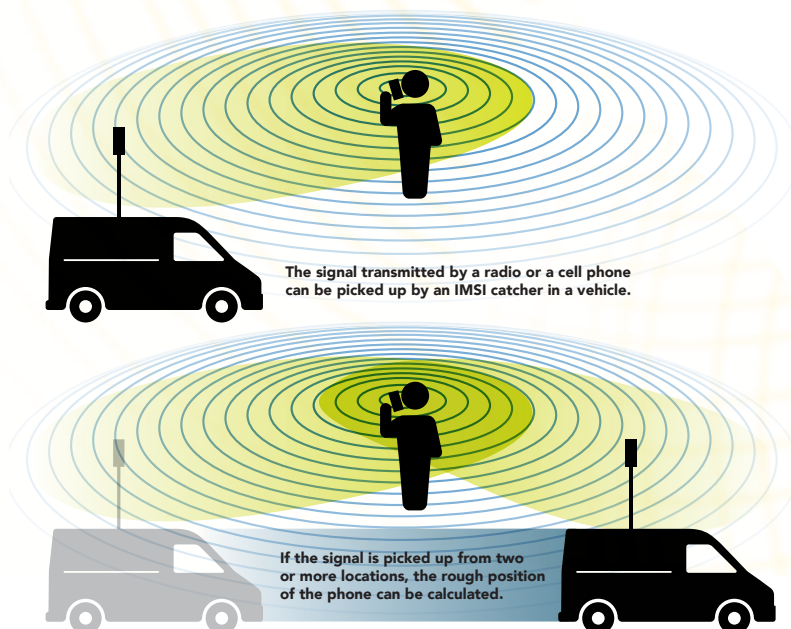
Another device for detecting and geolocating wireless signals is the T-Pod, made by U.K.-based BAE Systems. It consists of several IMSI catchers in a pod and is used on piloted aircraft as well as Reaper drones but is too heavy for a Predator to carry.[69]

One U.S. manufacturer of IMSI catchers, Florida-based Harris, sells its Stingray to dozens of police forces around the country, according to documents uncovered by the American Civil Liberties Union.[70] Other Harris devices include Gossamer (a small hand-held device), Hailstorm, Kingfish, and Triggerfish, which retail for as much as $169,000, together with special antennas and amplifiers named Amberjack and Harpoon respectively.[71]

Finding your location with a phone

Smart phones typically contain two radios. In addition to the receiver/transmitter that works on GSM or CDMA networks and allows users to exchange calls, text messages, and other data via local mobile phone towers, a smart phone also has a one-way GPS receiver that helps the phone locate itself.

The Global Positioning System (GPS) is an array of 31 satellites that orbit the earth and regularly send out two indispensable bits of data: each satellite's exact location and an exact timestamp, maintained by synchronized atomic clocks within each GPS satellite. [72] Thus anywhere on Earth, a smartphone can pick up at least three such satellite signals to mathematically calculate its position accurately using trilateration—a more sophisticated version of triangulation. Newer phones combine GPS data with local WiFi signals, local mobile phone tower data, and even Bluetooth to calculate locations faster. [73]

GPS GLOBAL POSITIONING SYSTEM

GPS devices pinpoint their locations by calculating where the signals from the closest satellites intersect.

Since a GPS device is only a receiver, *i.e.* for a user – be it a phone owner, a vehicle or a drone – to find their own location, it is not able to transmit its location to anyone else. However, when a smartphone user enables location sharing, this GPS data can be shared with apps via the second radio in the phone and used to calculate directions or nearby places of interest from cached databases. And while GPS location data could theoretically be hacked, this does not affect most users in Afghanistan and Yemen who have not historically used smartphones or GPS devices.

E: Relaying The Data

Data transmission problems have plagued the U.S. military since the start of the so-called "War on Terror," not least because drones take up significantly more bandwidth than piloted planes. For example, just one Global Hawk drone , on average, requires five times as much bandwidth as the entire U.S. military did during the 1991 Gulf War. There simply aren't enough government satellites to support this increase.[74]

In addition to dispatching near real-time surveillance video, for instance, drones must transmit video from the nose of the aircraft so that pilots on the other side of the world can control them. They must also send data like wind speed, location, and direction.

Two kinds of transmitters are mounted on the typical Predator or Reaper. The first operates in the C-band of the radio spectrum and is used by the Launch and Recovery Element (LRE) crew who control the aircraft as it takes off or lands at its local base—at Camp Lemonnier, Djibouti, for example, where drone operations over Somalia and Yemen are based. [75] This C-band radio is limited to about 170 miles around the local base because it uses line-of-sight transmission. [76]

The LRE crew hands the drone over to a U.S.-based Mission Control Element (MCE) crew after takeoff and takes control back before landing. [77] For this, the MCE crews rely on the second transmitter that communicates in the Ku-band of the radio spectrum via satellites. But

Drone satellite antenna.
CREDIT: Tom Tschida, National Aeronautics and Space Administration.

the data take about a second to travel from the U.S. to a drone over Yemen, so pilots must factor in the lag time, or "latency," when sending commands to control the drone or fire its missiles. [78]

Drone bandwidth is measured the same way as internet connection speed: via the amount of data that can be transmitted per second. The original MTS-A sensor ball, for example, transmits analog-quality video that requires significantly less bandwidth—1-3 Mbps. The MTS-B, Raytheon's second-generation sensor, captures video at higher resolutions that require a 3-10 Mbps connection. [79]

Ultimately data transmission depends on the same factors that determine how well a wireless internet connection works:

» **Capacity**, or how much data can be transmitted. This factor depends on both the speed a drone can upload and that a satellite can receive data. Older Milstar satellites provided a

maximum of 1.5 Mbps throughput, which increased to 8.2 Mbps with the launch of the Advanced EHF satellites. [80]

» **Congestion,** or how much bandwidth is available at a given time. The principle is the same as when multiple users connect to a household WiFi router and start streaming movies, causing the connection speed for each user to deteriorate.

» **Obstructions,** such as rain, dust, lightning, and mountains can disrupt data transmission.

For an analyst to identify details like whether an individual is wielding an object the size of an AK-47 rifle, drones need to transmit video at 45 Mbps. Smaller weapons like pistols require a much higher data rate. (By comparison, in 2010, the peak year for drone strikes, the average U.S. home internet speed only 3.9 Mbps) [81]

To support the drone war, the military now relies on bandwidth from commercial providers like Eutelsat, Inmarsat, Intelsat, and SES Government Solutions which can steer satellites to provide spot beams of high-speed data on demand.[82] Beginning February 24, 2012, the U.S. launched five new Lockheed Martin Mobile User Objective System (MUOS) military satellites to increase capacity. [83]

To overcome the mountainous topography in areas like Afghanistan, the U.S. also operates piloted aircraft such as Bombardier jets that fly in circles at 55,000 feet and above. [84] These aircraft carry a Battlefield Airborne Communications Node (BACN), a data relay that can pick up weak transmissions from individual drones or ground troops and relay them to other users and to military bases in the local network.

SATELLITE RELAY

MISSION CONTROL ELEMENT (NEVADA)

LAUNCH & RECOVERY CREW
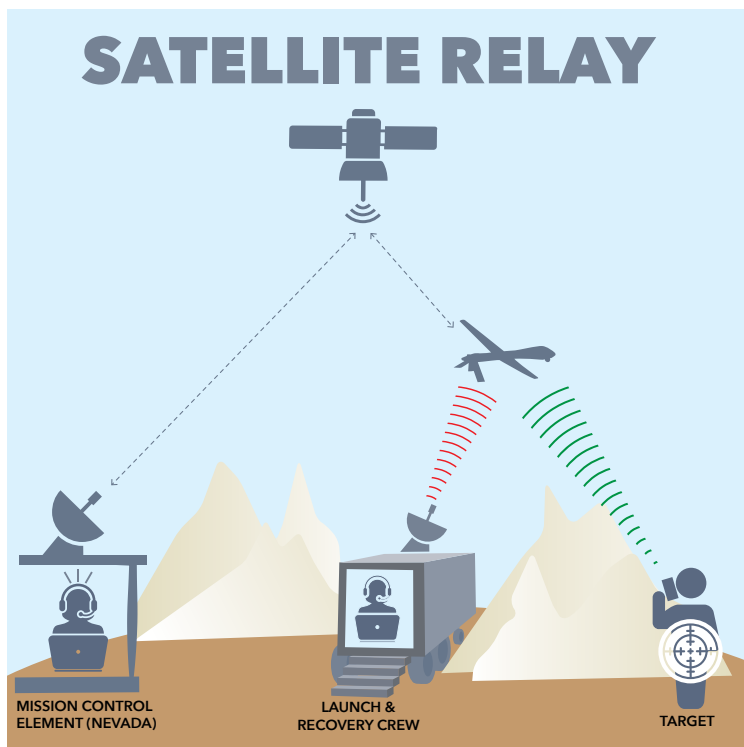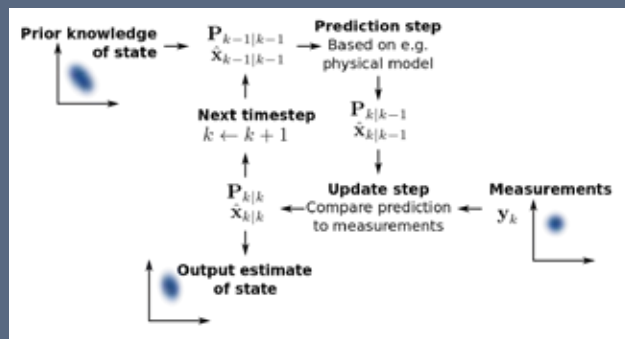
TARGET

SOFTWARE
Identifying Targets

ALGORITHMS 101

"We're going to find ourselves in the not too distant future swimming in sensors and drowning in data," Lt. Gen. David Deptula, Air Force deputy chief of staff for intelligence, surveillance and reconnaissance (ISR), told a 2010 conference.[85]

That prediction may already have been overtaken by events. In a 2008 study of sensor-collected intelligence, two years before Deptula's assessment, the Defense Science Board concluded: "Large staffs, often numbering in the thousands, are required in theater to accept and organize data that are broadcast in a bulk distribution manner. These analysts spend much of their time inefficiently sorting through this volume of information to find the small subset that they believe is relevant to the commander's needs rather than interpreting and exploiting the data selected on current needs to create useful information."[86]

Kalman filter illustration. CREDIT: Petteri Aimonen.

To sort through this haystack, the military has turned to algorithms. An algorithm is basically any sequence of actions used to solve a problem or to complete a task to make complex and repetitive tasks easier. Algorithms are typically applied to computer problems or tasks, but are widely used in many aspects of our daily lives today.

"In areas ranging from banking and employment to housing and insurance, algorithms may well be kingmakers, deciding who gets hired or fired, who gets a raise and who is demoted, who gets a 5 percent or 15 percent interest rate," writes Frank Pasquale, a law professor and the author of the book, *The Black Box Society*. "People need to be able to understand how they work, or don't work. The data used may be inaccurate or inappropriate. Algorithmic modeling or analysis may be biased or incompetent."[87]

In the world of drones, multiple algorithms have been unobtrusively embedded in the sensors as well as in the targeting technologies. Ultimately, these algorithms can help decide who lives and who dies.

Most algorithms are fairly generic. The accuracy of the results they produce depends on a variety of factors beginning with the quality of the data they receive, the assumptions behind those data, how the data are weighed, and the "learning model" by which they are trained to filter out wrong answers.

While algorithms can identify patterns from a sea of data, the more complex or dirty the data is, the more rules and data "attributes" an algorithm needs

to accomplish a task. A simple example might be to show a computer multiple images of trees and tanks, and then ask it to count the number of tanks and trees in a new photograph. Likewise, one might ask a computer to identify "men with guns" after feeding it pictures of guns.

Just like humans, algorithms improve when they are taught well and get lots of practice. Thus an algorithm that has been trained on 100 different pictures of guns will probably be more accurate than an algorithm that has studied only 10.

The accuracy of an algorithm can be measured by looking at the false-positive rate (the number of times it mistakenly counts men without guns as men with guns) and the false-negative rate (the number of times it counts men with guns as men without guns). While an algorithm can be trained to improve its false-positive and false-negative rates, there will always be circumstances that can trip it up, such as a target who wraps a blanket around his guns, or someone holding firewood.

Here, to set the stage before we delve into the specific technologies and their drawbacks, are four examples of key algorithms used by the Pentagon in the drone war. The first two are motion planning algorithms: the Kalman Filter and the Interacting Multiple Model filter; the third is Random Decision Forests, a learning algorithm; and finally, Greedy Fragile, a targeting algorithm.

Take the Kalman filter. It was first invented in 1960 to predict variables in a system that is continuously changing, such as a flying plane. The algorithm estimates the current state of the system based on data from previous points in time. It also estimates the uncertainty in the system and seeks to filter out "noise" or useless information as well

as random or inaccurate information, by giving them lower weight or importance in the final estimates. The most famous use of the Kalman filter was to predict the real time path of the Apollo space missions. Now it is widely used across a range of disciplines.[88]

In 1988, two researchers invented a way to combine data from multiple sources, each of which could be changing at the same time. They named this new algorithm the Interacting Multiple Model (IMM) because it allowed for multiple different Kalman filters to be checked against each other for weight or importance.

IMM is used for predicting aircraft traffic as well as target tracking by drones using radar, video, and geolocation data. Today Henk Blom, one of the inventors of IMM, is professor of Air Traffic Management Safety at the University of Delft in the Netherlands. Yaakov Bar-Shalom, the other inventor, has taught classes at the Pentagon and published papers including "Multi-Sensor Multi-Target Tracking" and "Target Tracking and Data Fusion: How to Get the Most Out of Your Sensors." [89]

In addition to tracking aircraft and drones, the Kalman and IMM algorithms are used to detect other moving targets like animals and people with lesser success, since living things are much less predictable.

Another key use of algorithms in the world of surveillance is to identify potential "terrorists" from big databases of information. To do this, according to documents released by whistleblower Edward Snowden, the NSA has used the common algorithmic learning tool, Random Decision Forests.[90] It allows a programmer to create smaller bundles of different data combinations and set up "decision trees" of yes and no answers.
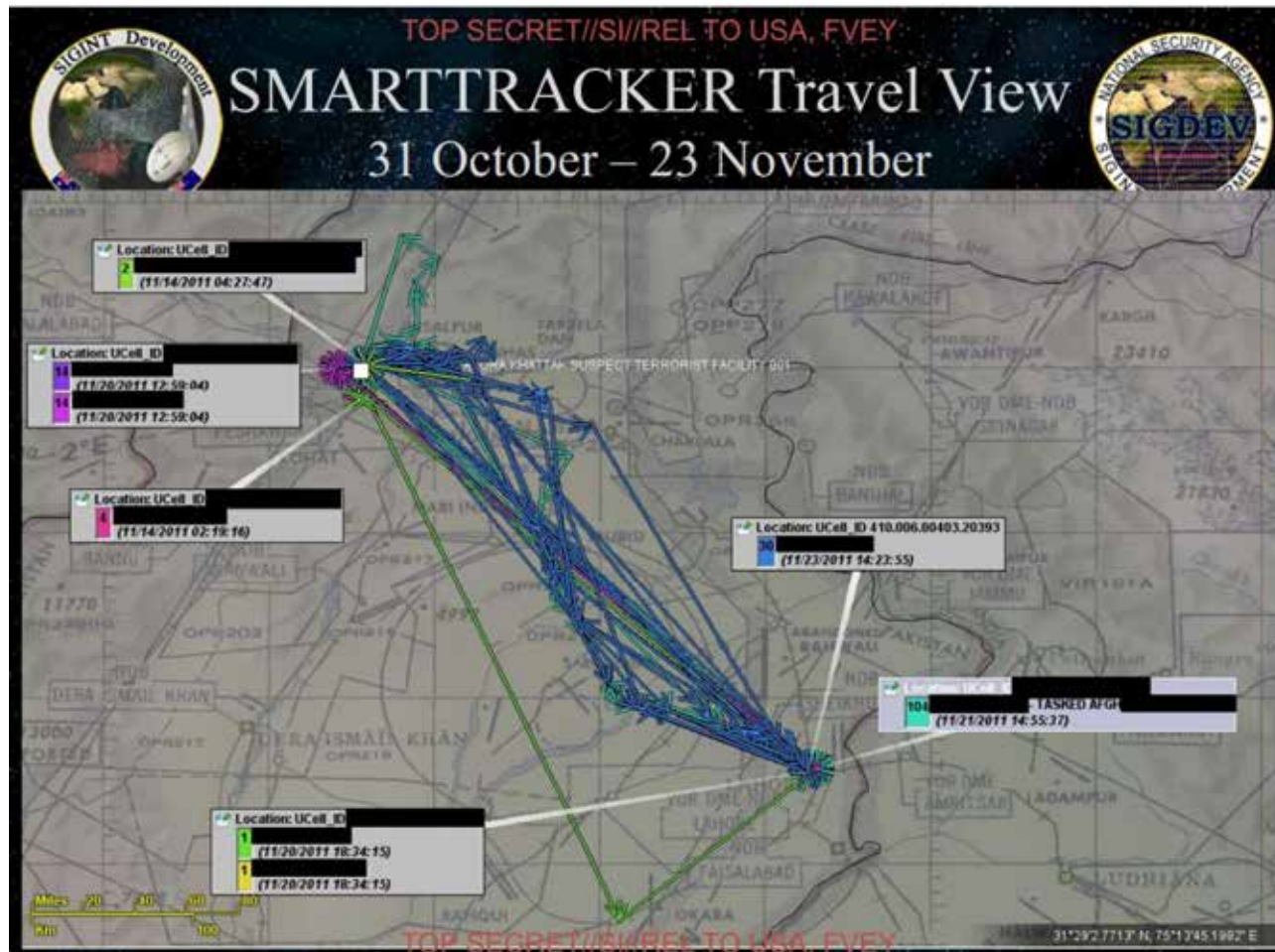
"Having created all those trees, you then bring them together to create your metaphorical forest," writes Martin Robbins in the *Guardian* newspaper. [91] "You run every single tree on each record, and combine the results from all of them. Very broadly speaking, the more the trees agree, the higher the probability is."

Our fourth example is Greedy Fragile, a targeting algorithm compiled in 2012 by Paulo Shakarian at the U.S. Military Academy at West Point. Shakarian wrote 30 lines of code that he claimed would help break up networks by attacking mid-level participants to make them more fragile.

"I remember these special forces guys used to brag about … targeting leaders. And I thought, 'Oh yeah, targeting leaders of a decentralized organization. Real helpful,'" Shakarian told *Wired* magazine. Zarqawi's group, for instance, only grew more lethal after his death. "So I thought: Maybe we shouldn't be so interested in individual leaders, but in how whole organizations regenerate their leadership."[92]

There's no public record that Greedy Fragile has been used for the drone program, but it is one example of military efforts to mathematically calculate whom to kill. Shakarian has created similar algorithms, like Spatio-Cultural Abductive Reasoning Engine (SCARE), for the military to help it track down roadside bombs in Iraq. [93]

Leaked Skynet presentation, National Security Agency. CREDIT: The Intercept.

F. Ground Moving Target Indicator

The Pentagon has been using basic tracking algorithms for a very long time, notably in radar systems that bounce radio waves off distant objects to "look" beyond the range of the human eye. In World War II, for example, Ford Instrument Company used algorithms in its primitive computers to aim missiles at enemy ships. [94] Such technologies allowed the Navy to hit targets it could not see. Radar algorithms are also routinely used to monitor intruders at airfield perimeters or enclosed compounds.

Targeting ships at sea and watching walls and gates are easy tasks, since large objects can easily be monitored against a relatively uniform canvas. But radar has a much harder time dealing with what engineers call "noise and clutter." When watching the ground from an overhead drone, tracking algorithms could be easily confused by sheep in a rural environment and by most moving objects in a complex urban area. [95]

In the Yugoslav war in the 1990s, for example, automatic target recognition (ATR) algorithms used to identify enemy tanks did not fare too well. "From our experience at three field exercises and a current operational deployment to the Bosnian theater, this is not the best way to get total system performance," a 1997 military study concluded. "The human operator makes decisions based on learning, history of past events, and

Radar imagery. CREDIT: Air Power Australia.

surrounding contextual information. Loss of these factors by providing imagery, latent with symbolic cues on top of the original imagery, actually increases the workload of the operator."[96]

The problems persist. "The ability of humans to discern targets is still significantly greater than that of electronic processing algorithms," James Ratches, the former chief scientist of the Army's Communications-Electronics Command Night Vision and Electro-Optics Directorate, wrote in a 2011 technical paper. "Full automatic target recognition may be unattainable, or at best, take a long time to mature."[97]

Despite this, drone crews rely on algorithms like Kalman and Interacting Multiple Model in Ground Moving Target Indicator (GMTI) software to help point a drone camera by tracking the paths of objects and people on the ground. David Fulcher, deputy director of the U.S. Northern Border Facility and an experienced Reaper pilot himself, explained why to *UAS* magazine in 2016. "The cameras are pretty small with a narrow field of view, It can't do wide-area collection at the same time," Fulcher said. "You have to know what you're looking for in order to be able to see it on the camera." [98]

For Fulcher's job—tracking people sneaking across the U.S. border—GMTI might seem like an ideal solution, given that he does not need to know the names, citizenship or the motives of the individual. Once the radar spots moving objects, a drone crew can zoom in with a camera. "You can pick out things like a group of smugglers coming across the border. You can tell how many there are. You can tell that they're carrying backpacks," Fulcher adds. Then all he has to

do is send out a Border Patrol team to arrest them and the legal system does the rest.

Yet a December 2014 assessment of the performance of a fleet of ten Predators used to police the U.S.-Mexico border for eight years, conducted by the inspector general of the Department of Homeland Security, declared that the program was a dismal failure. [99]

In Arizona, Customs & Border Patrol (CBP) estimated that the Predators contributed 1.8 percent of all arrests, and in Texas, they helped in just 0.07 percent. "Although CBP anticipated increased apprehensions of illegal border crossers, a reduction in border surveillance costs, and improvement in the U.S. Border Patrol's efficiency, we found little or no evidence that CBP met those program expectations," the inspector general wrote.

Ground Moving Target Indicator Vendors

GMTI software often comes bundled with synthetic aperture radar systems. One of the companies that provides GMTI software for Predator and Reaper drones is Australia-based Sentient Vision Systems, which sells a product called Kestrel. "We reliably detect targets down to two-by-two pixels in size, but with proven performance down to a half pixel in certain conditions," Tom Loveard, Sentient's chief technology officer claimed to *Tactical ISR Technology*. "Kestrel watches every pixel, hour after hour, and enables operators to concentrate on detected targets, rather than draining their focus with the base search task."[100] Northrup Grumman and RadiantBlue of Florida also develop and sell GMTI software for use on drones. [101]

G. Geolocation

Target phone tracking also uses algorithms. When an IMSI-catcher detects phones within range, it simply indicates that a device is located within a given radius. But for observers to exactly locate a mobile phone user requires certain methods, most of which use multiple, geographically separate sensors and calculation algorithms.

Drones and other surveillance aircraft carry IMSI-catchers that collect information about intercepted signals like the direction, or angle, it arrived from, the exact time it arrived and the signal's frequency. Each measurement provides valuable information for calculating the estimated location of phones.

The most common geolocation method is called "direction finding." It relies on the first measurement described above, "angle of arrival." That angle is measured at different sensors, or at the same moving sensor as it "hears" the signal at different locations over time. Straight lines are then drawn out toward the point where the signal came from, and where those lines intersect is believed to be the location of the phone or radio. Algorithms performing this calculation can be as simple as plotting those lines on a map or using least-squares error estimation and discrete probability density methods.[102]

A more novel, and problematic, method of geolocation is known as Time – or Frequency-Difference-of-Arrival (T/FDOA), which calculates the location

National Reconnaissance
Office logo.

of a phone or radio based on the difference in arrival time or signal frequency as measured at different sensors.[103]

The resulting estimates can only be approximate because the drones are moving, and often the phones are too. Indeed, all geolocation methods rely on relative measurements — estimating where the phone or radio is in relation to the known locations of the sensors. Accuracy therefore drops with "positioning errors (how well the aircraft knows its own position), signal measurement errors (how well the receiver can capture the received signal), and noise inherent in the signal," Kimberly Hale, an Air Force research analyst, writes in her 2012 Pardee Rand graduate school PhD dissertation on drones and geolocation. [104]

For example, pilots rarely have an exact lock on the location of drones since their on-board GPS can only provide latitude and longitude, but not the drone's exact altitude or the angle of travel. A drone with a badly calibrated gyroscope (used to stabilize the aircraft) or a relay satellite that has drifted even slightly off course can throw off calculations, as can a phone signal that has bounced off buildings or mountains.

Locating the sources of radio signals has long been a military goal. Guardrail, one of the key predecessors of modern phone
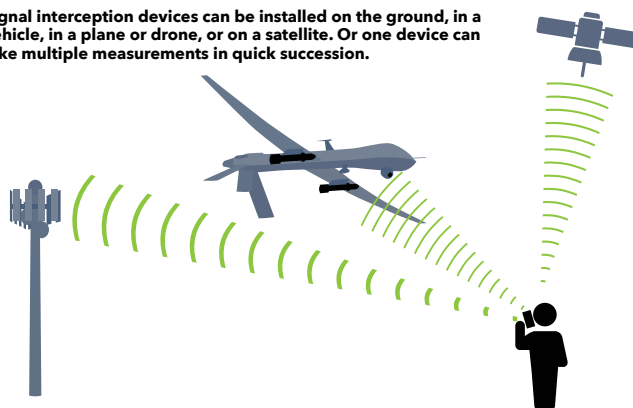
GEOLOCATION

1 Phones, walkie-talkies and laptops use radios to communicate. The signal they emit goes as far as it can in all directions like ripples from a pebble dropped in water.

2 A radio can be located by measuring the signal from at least three different known locations, ideally at the exact same time, and figuring out where the measurements intersect.
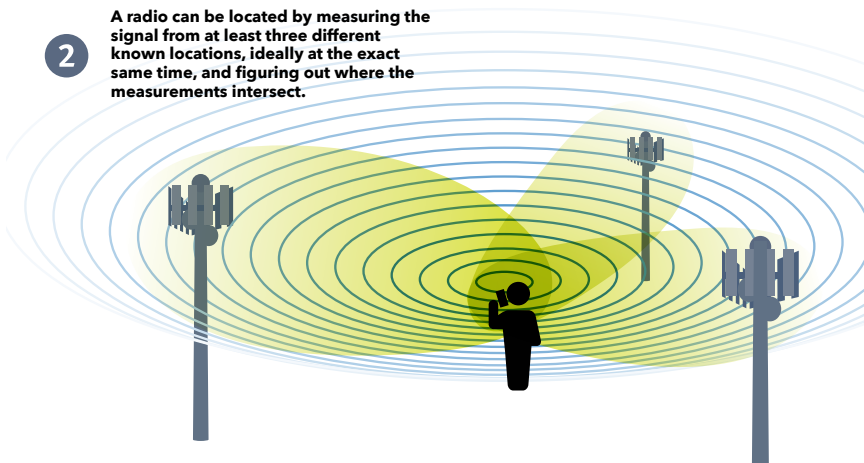
3 Signal interception devices can be installed on the ground, in a vehicle, in a plane or drone, or on a satellite. Or one device can take multiple measurements in quick succession.

4 If either the interception device or the target device is moving, the calculations are more complex.
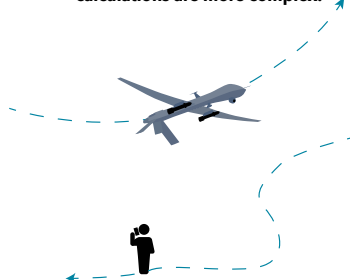
5 When signals bounce off buildings or mountains they make calculations harder. Weather can also disrupt signal measurement.

SOFTWARE

geolocation systems, was first used in Germany in 1971 to monitor Soviet troop movements in Eastern Europe. Still in use today, Guardrail employs three piloted Beechcraft C-12 Huron aircraft flying in orchestrated patterns to intercept selected low-, mid-, and high-band radio signals.[105] Data from the three aircraft are sent back to ground stations, which then calculate the location of the "emitter."

Unfortunately, flying multiple drones in orchestrated patterns is not easy when the pilots are on the other side of the world. Rather than rely on three imperfect drone readings, then, analysts sometimes request help from the National Reconnaissance Office's (NRO) dedicated military satellites.

The details of such support are not public, but there is some evidence it might come from a secretive program: Airborne Overhead Cooperative Operations (AOCO).

"AOCO helps … provide the warfighter with near real-time, enhanced geolocations on high-priority tactical missions," Frank Calvelli, the NRO principal deputy director, told a U.S. Congressional hearing in March 2016.[106] "In 2015, AOCO improved geolocation accuracy by 75 percent over single sensors, and reduced specific mission planning analysis times by 90 percent." An NSA document leaked by Edward Snowden and published in the *Intercept,* also suggests that the NRO's Mission 7600 satellites can collect phone locations.[107] (These satellites also help spy on Middle East internet cafes, which rely on VSAT dish systems. In places where mobile data is slow, these cafes are sometimes the only way to get online.)

Modeling A Better System

Literature on the accuracy of drone geolocation of phones is somewhat sparse because of the clandestine nature of this kind of research. (By comparison, drone hobbyists have easy access to video, radar and infrared technology, and thus to data.) But it is clear from publicly available military research that one drone, flying alone, cannot reliably track mobile phones below.

Kimberly Hale, who now works as an operations research analyst for the Air Force, provided some insight in her 2012 master's thesis for the Rand Corporation. She said that the military needed to upgrade its drone fleet to T/FDOA (time/frequency-difference-of-arrival)[108]

The accuracy of such a system, Hale writes, will increase with the number of drone patrols used to gather signals. For example, a system of 10 combat air patrols (a minimum of 20 drones) flying at 15,000 feet can track only 20 targets in a country the size of Afghanistan with an accuracy rate of 25 percent. But Hale believes that if the Pentagon could simultaneously fly a minimum of 40 drones (20 combat air patrols) in complementary orbits at 30,000 feet, the Pentagon could reach 95 percent accuracy over Afghanistan.

Even this estimate comes with several caveats, the first being that Hale assumed for purposes of her calculations that Afghanistan was flat. Second, it should be remembered that the higher a drone flies, the lower the quality of the video signal. So the advantage of higher altitude tracking would have to be weighed against the disadvantage of not being able to see the targets. Not least is the significant number of drones

needed to fly simultaneously in order to ensure accuracy under Hale's plan.

Turkish military officer Volkan Tas took a more practical approach in his final thesis for a masters degree in electronic warfare systems engineering at the Naval Postgraduate School in Monterey in 2012. Tas tried to create a mathematical model using geolocation technology to help track Kurdish rebels in the mountains.[109]

"Civilian and military intelligence has been used at the strategic level to locate [Kurdish forces], but without operational and tactical location systems, success is fleeting at best," Tas writes. "The system should include at least four stationary and one flying UAV [drone] as the fifth receiver for better accuracy."

The problem with this approach is that it needs direct access to ground monitoring sensors, which may not always be available to U.S. troops in Pakistan or Yemen. (For example, the Waziristan mobile network is often turned off.)[110] If dedicated interception devices are installed at convenient locations or even mounted on vehicles, this method may work but it will still not be 100 percent reliable.

It should be noted that Predators and Reapers do not carry equipment on board to calculate the location of a phone. Instead this task has to be conducted on the ground by computer systems powerful enough to crunch the data using algorithms like the Interacting Multiple Model to correct for errors in each measurement.

Aware that phone location technologies are only approximate, senior intelligence officials have sought to improve accuracy. A 2009 lawsuit by Netezza,

settled out of court, sheds some light on one way the CIA has used complex algorithms to try to pin down target locations. [111]

Netezza

On September 15, 2009, CompSec, an obscure company in McLean, Virginia, placed an order for Netezza GeoSpatial, a new million-dollar computer system to be delivered to a U.S. government warehouse in Springfield, Virginia.[112]

Netezza, a multi-million dollar information technology business founded in Massachusetts, sells high-end hardware together with specially configured software. Its on-call technicians provide support and maintenance. While still in development, the new GeoSpatial product had reportedly undergone trials with Japanese mobile phone data and was considered a good fit for other major customers like Canadian Railway and the Dish Network satellite TV which had been shown "proof of concept" versions. [113]

Slide presented in IISI v Netezza lawsuit.

GeoSpatial was advertised as being able to pinpoint the precise location of users from extremely large data sets stored on Netezza's new TwinFin hardware. "Until now, decision makers and business users have constantly tried to answer 'who,' 'what,' and 'when' with respect to industry trends, customer and target demographics," declared a Netezza brochure marked "confidential" that was sent to potential clients. "Imagine if the 'where' component of every piece of data could be added." [114]

CompSec was just a go-between for a top secret client—the CIA—which was in a major hurry. "A gentleman named Skip McCormick from the CIA asked us if there was anything we could do to accelerate the development of this," James Baum, the Netezza CEO, would later recall in an April 2010 court deposition. [115]

McCormick sent Baum an email urging Netezza to speed up its work. "We just upgraded to a [Netezza TwinFin server], but it doesn't yet have the Geospatial tools," the CIA staffer wrote on October 14, 2009. "I'm trying to figure out what options are available for getting them asap. We depend on the Geospatial tools here every day." [116]

The problem was that Netezza didn't make the software the CIA wanted, but hoped to re-sell the spy agency a proprietary geospatial package made by Intelligent Integration Systems (IISi), a small Boston-based company. This software had been licensed to the bigger company for use on the older Netezza Performance Servers but was discovered not to work on the newer TwinFins.

Customers for the original IISi software included Foxwood Casino and the Democratic National Committee which used the software to track gamblers and voters respectively. [117] Rich Zimmerman, one of the company's co-founders, explained in a court affidavit that the software was designed: "to incorporate and cross-reference vast amounts of business data with geographic location within the same database, and enable events (such as a tornado heading towards a population center or a mobile phone signal moving from one tower to another) to be matched with personal characteristics in the database (such as telephone numbers for houses in the path of the tornado or the identity of the person whose mobile phone signal has moved from one tower to another) to be mapped and analyzed quickly and efficiently." [118]

This IISi software was really a business tool to figure out the identity of a user, not a geolocation tool. So when Netezza erroneously marketed the software to the CIA for the drone program, the smaller company balked. "My reaction was one of stun, amazement that they [the CIA] want to kill people with my software that doesn't work," Zimmerman stated in a court deposition. [119]

Netezza claimed that IISi had reneged on the terms of the software license, which stated that they would provide technical support. "It was clear that Netezza's claims were a fabrication—an outright, reprehensible lie," Marshall Peterson, another co-founder of IISi, wrote in an email to Baum and Zimmerman. Peterson, a decorated helicopter pilot who served three combat tours in Vietnam, was one of the developers of a supercomputer named Red Storm, designed for the Pentagon. He had also worked on the development of software for the human genome project. [120]
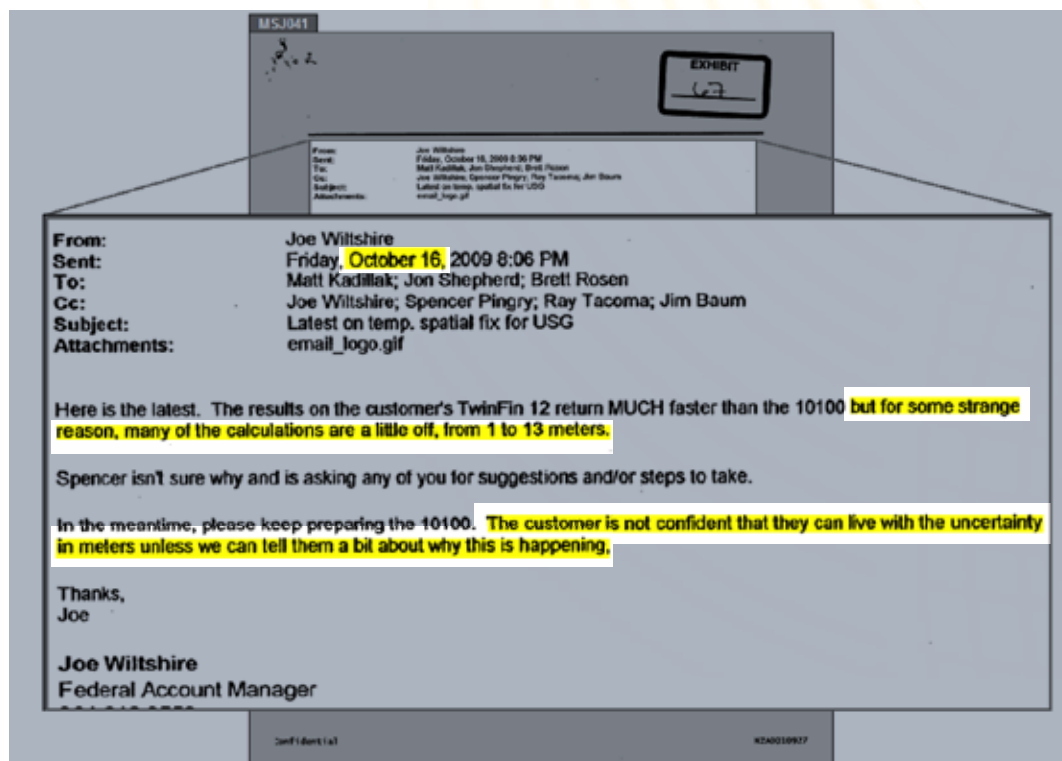
Slide presented in IISI v Netezza lawsuit.

The court documents show that Netezza executives and engineers panicked. "No matter how you slice this, we are screwed," Baum wrote to one of his colleagues. [121] The Netezza CEO noted that the company had sold $40 million worth of hardware and software systems to secret, unnamed U.S. government clients in the past year. He was loath to fail on this project, given that Netezza was projecting it could expand federal sales to as much as $100 million the following year. [122]

Then IISi sued Netezza, claiming that the new GeoSpatial product was nothing but an altered version of the IISi software—and that it violated the licensing agreement which stated that Netezza would not be allowed to make any changes to the source code. [123]

In other documents submitted to the court, Matthew Kadillak, a Netezza engineer, testified that he "frequently worked with the government customer in question" and that he helped complete the rush version of Netezza GeoSpatial that was delivered a few days later. [124]

But tests conducted in mid-October by Sri, an engineer working for McCormick at the CIA, soon concluded that the software could be off by as much as 13 meters (43 feet). [125] By November, Kadillak reported that he, too, was suddenly "seeing lots of errors." [126]

The two companies came to a confidential out-of-court settlement in November 2010 to drop the lawsuit, soon after IT behemoth IBM bought Netezza for more than six times its expected revenue that year.[127]

H. Cross Sensor Cueing

With the bewildering amount of raw data streaming back from multiple sensors on drones, and an array of tools to analyze the information, the Pentagon has been working to simplify and automate target selection. While truly autonomous artificial intelligence systems are still many years away, these new target selection systems are helping remove humans from the killing process.

The Air Force Research Laboratory at the Wright-Patterson Air Force Base has an entire division of research scientists whose task is "sensor management" and the development of "cross sensor cueing" systems that can combine data from multiple sensors to help automatically "cue" *i.e.*, direct aircraft, point video cameras, and launch missiles. [128] One such system is the Network Centric Collaborative Targeting System (NCCT), built by ComCept, a division of L-3 Communications. [129]

The company explains: "ComCept's multi-intelligence/multi-platform sensor networks greatly accelerate the find, fix, track and target portions of the kill chain, including rapid location of short up-time emitters and tracking of fleeting high-value targets within the target window of vulnerability. Our expertise in data modeling with scalable, distributed network configurations allows for rapid integration of new sensors and capabilities into a common network supporting near real-time tasking and

machine-to-machine sensor cross-cueing." [130]

In essence, this means that when an individual on a wanted target list briefly turns on a listed mobile phone, and as soon as overhead drone or a land tower picks up the phone's signal, the NCCT system can rapidly send a message to the closest drone video camera and point it toward the phone. An imagery analyst watching this video feed would not necessarily know what technology, systems, or people were involved in tracking the device.

One principal challenge in building such a system was the fact that different types of sensors collect different types of data, meaning that each sensor essentially speaks a different language and cannot communicate outside of that language.

Gen. John Jumper.
CREDIT: Jim Varhegyi, U.S. Air Force.

To solve this problem, the Air Force threw out a challenge to come up with a common standard that everybody could use without abandoning their existing systems. "The sum of all wisdom is a cursor over the target," Gen. John Jumper, then Air Force chief of staff, told the attendees at the April 2002

CROSS SENSOR CUEING

COMPUTER TARGETING

POSITIVE ID! · FIRE!

HUMAN TARGETING

ERROR? · NEGATIVE ID! · STAND DOWN!
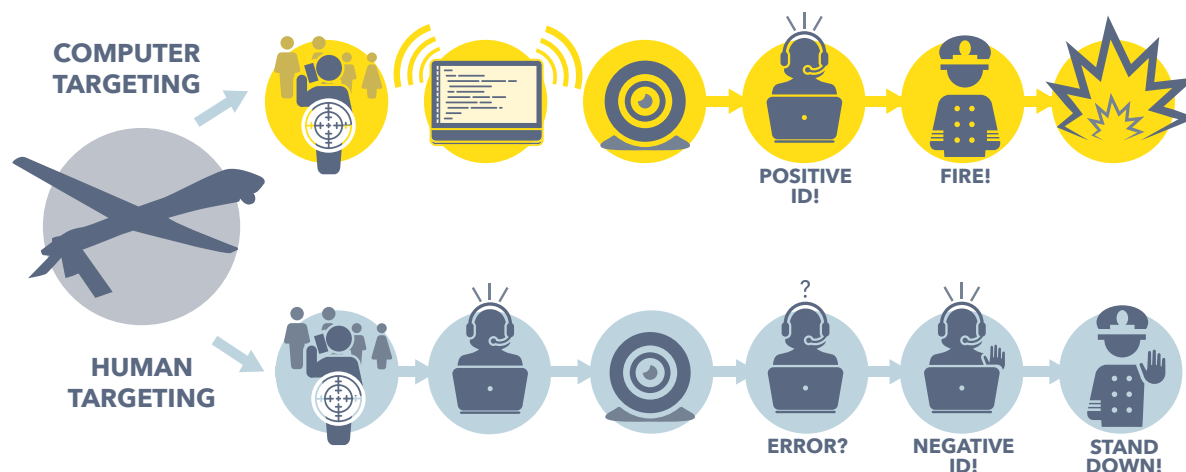
Command and Control, Intelligence, Surveillance and Reconnaissance conference.[131]

Jumper's remark became a mantra: cursor-on-target or CoT for short. It spawned a new uniform data standard to focus multiple sensors on one mission by reducing all targets to just three key variables: what, where, and when. This new standard spawned new software contracts (notably with MITRE Corporation, a Virginia-based, government funded non-profit), academic papers, and even entire conferences. [132]

This CoT methodology made it easy for algorithms to identify targets and spare human operators the laborious work of comparing multiple kinds of sensor information, such as video, thermal, and phone location data.

But to do this, systems like cursor-on-target oversimplify the problem, throw out any contradictory data, and can end up creating a cart-leading-the-horse approach: They define a target in order to take it out, rather than assess whether the target is even the correct one. This strategy risks producing what statisticians call **confirmation bias**: the tendency to interpret evidence as confirmation of an existing theory or conclusion.

Ticom Geomatics

Some of the key technology for cueing sensors is made by Ticom Geomatics, a small Austin, Texas start-up founded by a group of scientists who had worked together at another Austin facility—Applied Research Labs, an Navy research facility. [133]

Ticom sells GEOnet, originally known as ISRnet, which is software that enables a single operator to control multiple

sensors from the same workstation, allowing these sensors to work together to geolocate a mobile phone or similar communications device.[134] The company specializes in networking sensors to perform the more complex geolocation method described above, T/FDOA.

"I'm a software technical lead working on an application that coordinates the operation of geographically distributed, heterogeneous sensors and other sensor networks," Steven Glicker of Ticom announced in a public email post to a World Wide Web Consortium discussion group in April 2006. [135] "We must insure that our application will operate with a wide variety of sensors and sensor networks, as well as provide an interface to our 'consumers' so they may make effective use of the overall sensing capability without having to deal with specific sensor details."

The problem is that the geolocation technologies, as we have discussed, can easily be off by several meters. Swapping mobile phone numbers and SIM cards is also common in many parts of the world; locating a phone may not locate the right individual. [136] Unless imagery analysts are aware of all these potential error factors leading to their camera being trained on an individual, they are likely to believe that the person in their crosshairs is the person on the kill list, regardless of their true identity.[137]

Ticom's software has been adopted by the Marines, Army, Special Operations Command and U.S. intelligence agencies.[138] This success has turned the company into hot property. In April 2012, a bigger company, Six3, bought up Ticom for some $60 million. Just 18 months later, CACI, the company made infamous for the interrogators it supplied

to the Abu Ghraib prison in Iraq, acquired Six3 for $820 million. [139]

An Engineer Speaks Out

How accurate is Ticom's geolocation software? Without access to an independent audit, it is hard to tell, but as in the case of Netezza, there is at least one engineer who claims that the algorithms are inaccurate.

On December 27, 2016, Bernard Henneberger, an engineer who previously worked for Ticom, filed the latest in a series of petitions in what has become a three-year court battle against his former employer. [140]

The lawsuit alleges two things. First Henneberger claims that he was cheated out of a million dollar stake in Ticom when it was snapped up by Six3 and then by CACI.

The second charge is much more ominous. "I have repeatedly warned Ticom [that] the company's geolocation technology" could be inaccurate. "This endangers national security and risks innocent lives," Henneberger wrote and offered to help design a fix. [141]

Henneberger, who has a master's degree in signal processing from the University of Houston, was employed for seven years for Lockheed Martin at the NASA offices in Houston where he worked on the Space Shuttle and the Hubble telescope. He went to work for Ticom in 1998, shortly after it was founded by his former co-workers at Applied Research Laboratories at the University of Austin, Texas.[142]

His filings include news clippings as a stark reminder of the gravity of his allegations. The first was a 2014 *Associated Press*
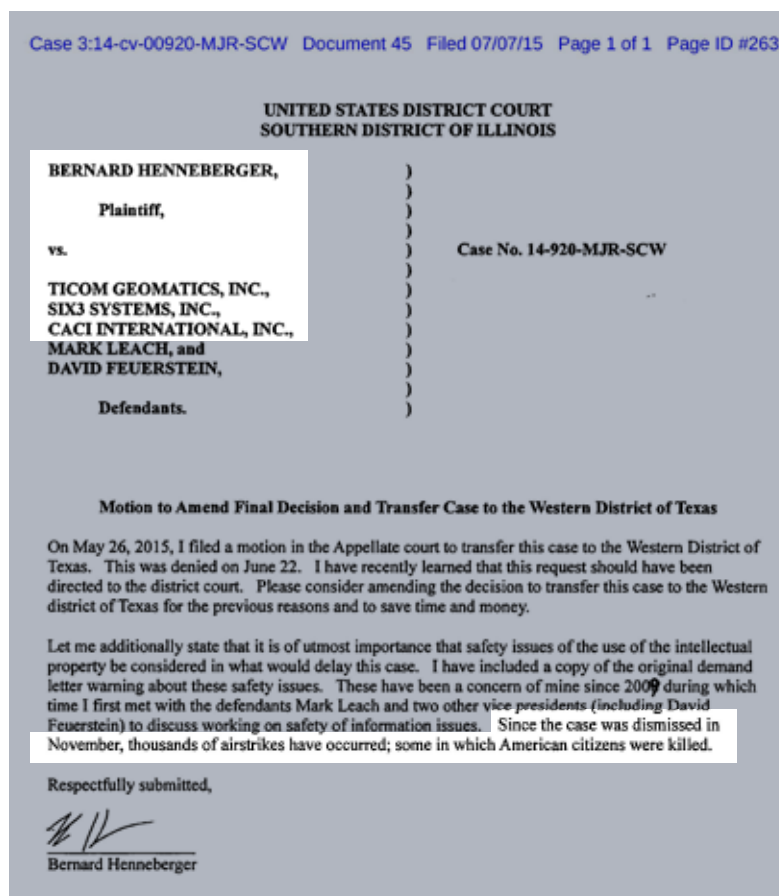
article headlined "Airstrikes launched amid intelligence gaps." [143] Henneberger later included the front-page copy of the *New York Times,* containing stories about the 2015 deaths of Giovanni Lo Porto and Warren Weinstein, two Westerners killed in a drone strike while they were held hostage in Pakistan. One of the attached articles is subtitled, "Drone Strikes Reveal Uncomfortable Truth: U.S. Is Often Unsure About Who Will Die." [144]

In interviews with CorpWatch, Henneberger confirmed the role of Ticom's technology, but, after talking to his lawyers, declined to provide any more details.

Henneberger v Ticom lawsuit filing.

I. Social Network Analysis

Battalion commanders are well aware that the inadequate quality of video, thermal imagery, radar data, and phone location systems aboard drones provide little more than a voyeuristic look at remote locations—even with motion detection and geolocation algorithms to help point cameras.

Instead, analysts rely heavily on human intelligence (such as interrogations and tips from sources) as well as social network analysis computer software that claim to offer a sophisticated way to spot suspicious connections between people.[145] Algorithms are applied to detect patterns inside the large quantities of raw data gathered.

Before the advent of these computer programs, the military conducted "link analysis."[146] Based on information derived from interviews, documents, and other intelligence sources, it involved physically sketching possible relationships between individuals. Results from such analyses are inherently subjective. They depend on the analyst's intuition as well as the quality of the original data. If any one source lies or errs, the entire map of relationships can be thrown off completely.

Social network analysis, by contrast, purports to provide objective answers. The idea is that patterns in large data collections can help provide a visual depiction of the person's objective importance within a given social network. Someone who is connected to many people may not be as important as someone who is connected to a few important people. The software also

SOCIAL NETWORK ANALYSIS
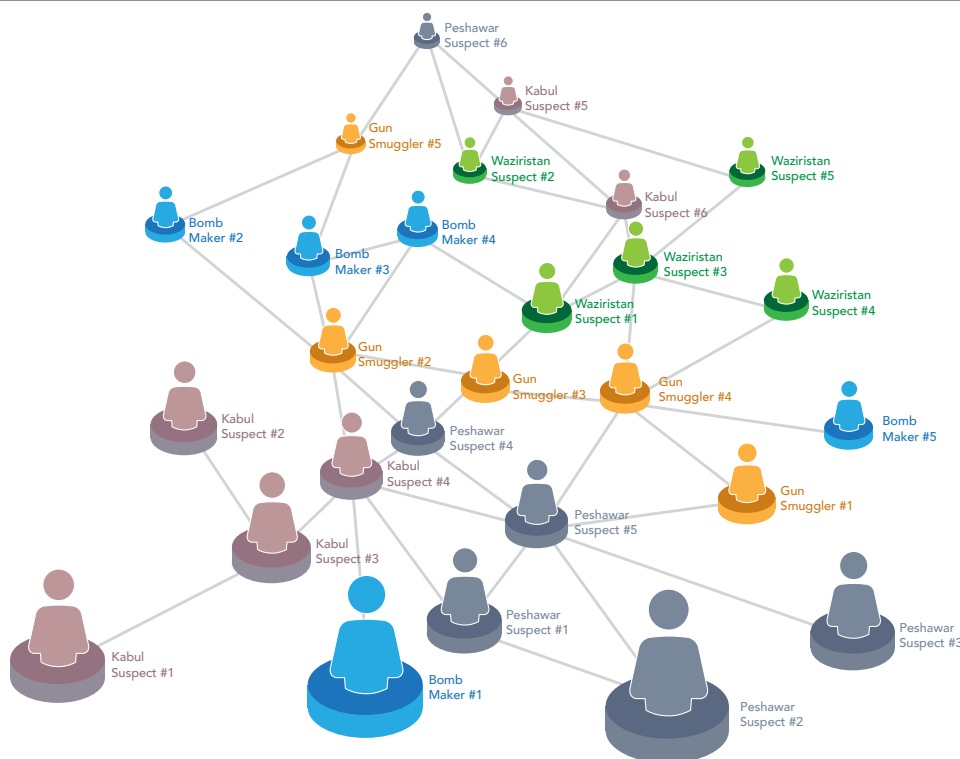
looks for factors like "betweenness" and "closeness."[147] By using social network analysis in combination with traditional link analysis, network experts like Vladimir Krebs say it is possible to "uncloak" a hidden network.[148]

After social network analysis has painted a picture of a network to be targeted, "pattern-of-life analysis" becomes a key technique to find specific targets. People perceived to be engaging in indicators of suspicious behavior are considered legitimate targets, and the analyst is assigned to see where they go, with whom they socialize, and other potentially suspicious activities.[149]

But unless the data set is verified, social network analysis and pattern-of-life analysis are prone to error and to confirmation bias (the tendency to use new data to support an unproven theory). After 2001, the NSA conducted social network analysis on U.S. phone records and other electronic communications metadata with the help of a secret program, "Stellar Wind."[150] It pinpointed common phone numbers believed to be central nodes in a possible terrorist network. Instead, the numbers often turned out to be takeaway food outlets, prompting the FBI to dub them "Pizza Hut cases." Bureau Director Robert

Mueller estimated that 99 percent of Stellar Wind tips "wash[ed] out." [151]

Despite these errors, such mapping is the military's main way to try to identify secret networks[152] within large populations. Tragically, when such methods are applied from a great distance, it becomes very easy to confuse two politicians or a reporter with a military target, even after correcting for blatant errors like the Pizza Hut example.

Two examples illustrate the confusion and its consequences.

The case of Muhammad Amin

Zabet Amanullah. CREDIT: Afghan Analysts Network.

On September 2, 2010, the NATO-led International Security Assistance Force (ISAF) in Kabul, Afghanistan, announced that a "precision air strike" had killed Muhammad Amin, a senior Taliban figure who was acting as shadow governor of Takhar province in northern Afghanistan. The military claimed that Amin and 8-12 other insurgents had been traveling in a convoy of six cars in a rural area. [153]

A jet dropped a large bomb on the car allegedly carrying Amin and his security detail. A helicopter gunship then swooped in to shoot other members of the convoy, some of whom were seen carrying weapons.

But Amin was not killed in the attack. He was tracked down later in Pakistan, where he was not only alive, but gave an interview to Michael Semple, a professor at Harvard University. [154] An investigation by the Afghan Analysts Network revealed that the convoy really belonged to an Afghan parliamentary candidate campaigning for upcoming elections. [155] The principal victim turned out to be the candidate's uncle, Zabet Amanullah, a well-known public and respected member of the local community.

Kate Clarke, a former BBC reporter, who personally knew Amanullah says that the U.S. military told her that an Afghan detainee in U.S. custody provided interrogators with a mobile phone number for Muhammad Amin, to whom the detainee said he was related.

Clark says that the military told her that they never verified the original claim. "They didn't do any background checks on either person. They had almost no knowledge about Amin and they hadn't bothered to get any knowledge about Amanullah," Clark told Andrew Cockburn, author of *Kill Chain*. [156] Had they watched local TV news broadcasts, for that matter, they could have quickly realized that the two men were different individuals.

Instead, intelligence analysts created a network map of the calls made by Amanullah—including some to the real Amin in Pakistan—and those made by the recipients of his calls. Not surprisingly, this network corresponded with some of the most important players in the province, given that the owner was, indeed, a prominent political figure.

But rather than following up in person, the U.S. military waited for a moment when they had a clear shot at Amanullah and then killed him.

The case of Ahmed Zaidan

Ahmed Zaidan.
CREDIT: Al Jazeera.

Ahmed Zaidan, the former Islamabad bureau chief for the Al Jazeera television network, grew up in Syria. A fluent Arabic speaker, he met Osama bin Laden in Kabul, Afghanistan, in November 2000, while on assignment as a reporter. [157] A couple of months later, he was invited to attend the wedding of bin Laden's son in Kandahar, on which he also reported on for the television network. After the U.S. invaded Afghanistan in 2001, Zaidan became one of the few recipients of Al Qaeda video tapes released over the next ten years, on which he also reported. [158]

Zaidan quickly became recognized as an expert on Al Qaeda and wrote the 2002 book, *Bin Laden, Unmasked.* [159] He was not the only writer to capitalize on such meetings with the Al Qaeda leader. Peter Bergen of the New America Foundation published *Holy War, Inc: Inside the Secret World of Osama Bin Laden* and *The Osama Bin Laden I Know.*[160]

In May 2015, *The Intercept* released a leaked NSA document that identified Zaidan as a "member of Al Qa'ida." The undated document explains how the SKYNET computer program examined some 80 variables like travel behavior, social networks and "patterns of life" from a trove of 55 million Pakistani mobile phone records that was gathered via an NSA collection program named Demonspit.[161]

SKYNET was trained by applying Random Decision Forests on 100,000 of these records. We don't know exactly what bundles that the NSA created, but hypothetically they might have combined data from phone calls between Karachi and Waziristan, together with the ages of the users. Another bundle might have joined together data on frequent travelers together with unusual patterns of phone usage.

Inside that group of 100,000, the NSA included seven individuals alleged to be terrorists. Since SKYNET had originally provided only six identities, the spy agency was ecstatic when the software identified the seventh.

But this method has come in for severe criticism. "First, there are very few 'known terrorists' to use to train and test the model," Patrick Ball, director of research at the Human Rights Data Analysis Group told the *Ars Technica* website. [162] "If they are using the same records to train the model as they are using to test the model, their assessment of the fit is completely bullshit. The usual practice is to hold some of the data out of the training process so that the test includes records the model has never

seen before. Without this step, their classification fit assessment is ridiculously optimistic."

Further compromising the model, the NSA assumed that none of the other 100,000 individuals were terrorists. In real life, if the training data contained such individuals, the NSA would effectively be training the algorithm to ignore them.

Zaidan condemned the analysis of his mobile phone calls. "It is interesting to point [out] that the document also mentioned that I have the telephone numbers of very important people," the reporter wrote on Al Jazeera's website. "Was I supposed to have the phone numbers, with all due respect, only of garbage collectors, for example? Am I supposed to only have the contacts of unimportant people?"[163]

Zaidan pointed out that the NSA analysis neglected to consider the obvious: It "ignored my taped reports on Al Jazeera television that showed where I was and with whom I was meeting between 2001 and 2011."

Last but not least, Zaidan pointed out that the analysis contained glaring factual errors: It claimed, for example, that he was simultaneously a member of al-Qaeda and the Muslim Brotherhood, which are sworn enemies.

It is still not clear if the NSA was using Zaidan simply as a case study on SKYNET or if it was convinced of his guilt. Either way, he has been luckier than Amanullah. As a member of the media, his innocence was vouched for by colleagues like Bergen. Still, deciding to err on the safe side after the document was leaked, Zaidan left Pakistan to work out of the United Arab Emirates.[164]

Graph Databases & Semantic Wikis

Many companies sell social network analysis tools to the Pentagon to help the government mine the vast silos of sensor and related surveillance data gathered on a daily basis. These "Big Data" tools attempt to quantify uncertainty in complex problems. While mathematicians and statisticians who design such tools are wary of promising that their data models can identify individual criminals or potential attackers, corporate sales departments at military contractors are not shy about hyping their wares.

Palantir is one of the best known companies in this field, but others, including Modus Operandi and Leidos, offer add-on tools like Halogen and Wisdom to analyze information from the open internet, the deep web and social media accounts.

One of the key products on offer is "semantic wikis" because users can edit and update them like Wikipedia pages. But unlike Wikipedia, which is a collection of static text pages connected via hyperlinks, semantic software also classifies information inside data sets and attempts to interpret them. [165]

To begin with, users regularly add new information such as field reports from soldiers, news articles, social media posts, sales and bank records, floor plans, maps as well as video and phone location records from drones. The software then maps, tags, and stores this information in "triplestore" databases (so named because they contain three elements: class, attribute, and value) or a "graph" database.[166]

The tagging is often done using natural language processing algorithms that examine the structure of words, phrases

and sentences and assign specific values to each "object" in the database. Critical to this kind of search is the definition of the relationships among the various objects in the database. [167]

In many ways, these graph and triple-store databases are a sophisticated version of Google which uses propri-etary algorithms to rank information and extract answers from vast databases of documents. The military databases, of course, have access to a parallel universe of classified data unavailable to public search engines like Google and Yahoo.

A major selling point of these tools is the ability to create multiple, different visual displays of stored data as a system of objects, properties and relationships to help military analysts—typically aged between 19 and 25—make sense of raw data from other countries, cultures, and languages and spot potential threats.

Modus Operandi

Modus Operandi, based close to Cape Canaveral in Florida, sells the military a product named Blade. [168] It offers a Google-like query system for soldiers to look up information in intelligence databases indexed using the company's Wave system and automatically generate tailored reports.

"If you input a new piece of informa-tion, like 'This guy has a connection to this organization,' that organization will appear on his page. And so you can click on that organization and it will take you to the page for the organization, then it gives you the links back to all the under-lying reports where the information in the graph came from," Eric Little, Modus Operandi's chief scientist told *Datanami*. "Our system connects dots. We actually make the data smart and we make the
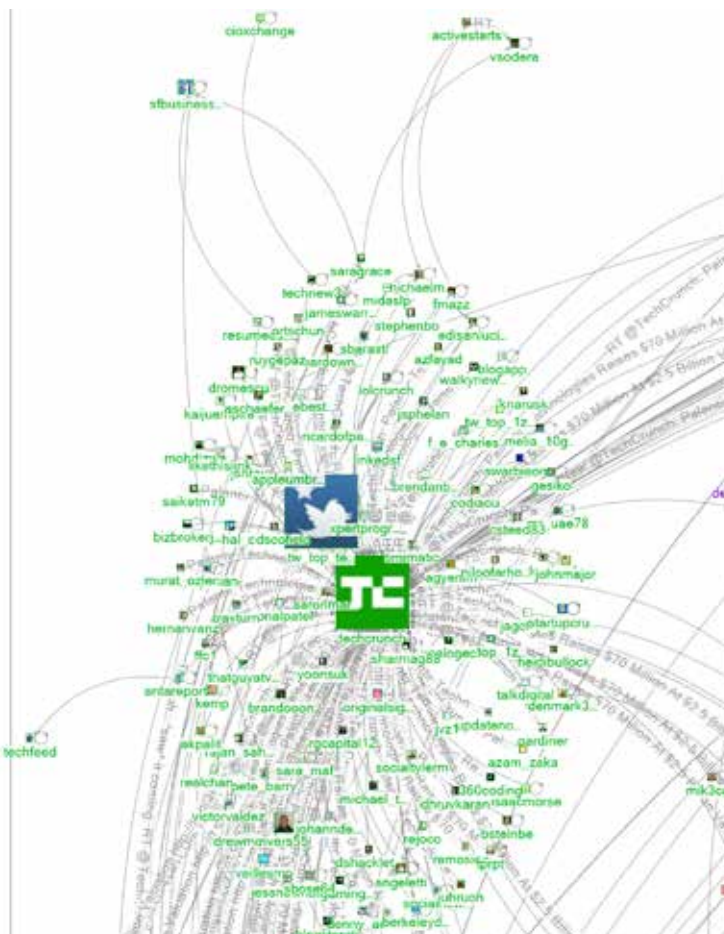
data easily consumable for people to actually use for real decision-making." [169]

Modus Operandi was awarded research contracts from the Navy to create wiki pages for military mobile devices called WISER (Wiki for Intelligent Semantic Event Reporting) and STAFF (Semantic Targeting and All-source Fusion Framework) to help track entities of interest and improve targeting effective-ness. [170]

Other research projects awarded to Modus Operandi include the Clear Heart project to analyze sensor data "to recog-nize adversarial intent in public areas," and POLIS (Pattern Of Life Integrated System) "to find behavioral patterns that may indicate mal-intent." [171]

Social media analysis of people who tweeted the word Palantir
CREDIT: Marc Smith.
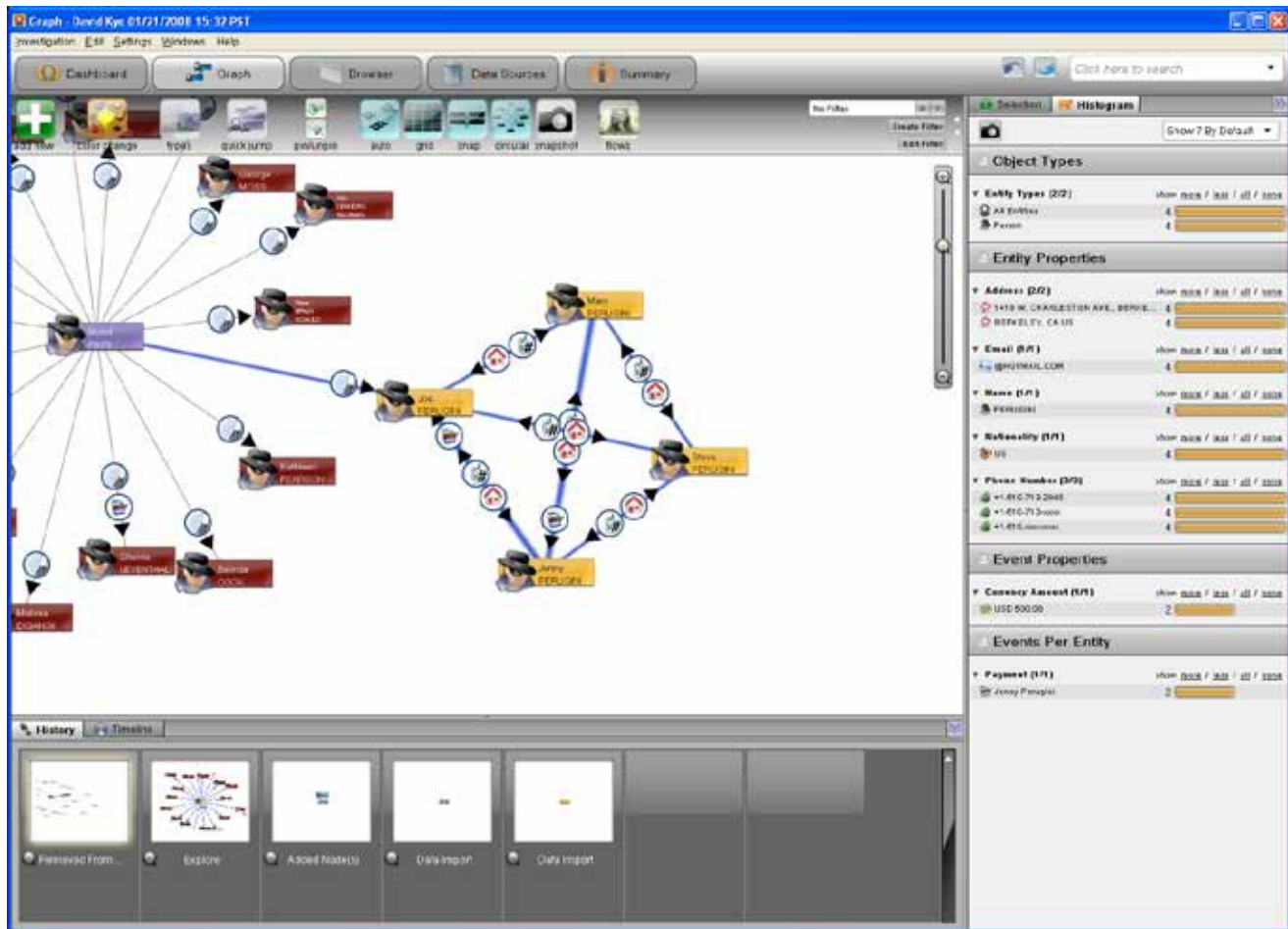
"By analyzing data from many different sensors, this system will indicate—with visual alerts—if something deviates from expected patterns," Peter Dyson, Modus Operandi CEO said in a press release about POLiS. "These red flags can be tremendously helpful in preventing malicious behavior in almost any setting, whether it's a war front or an urban environment." [172]

Modus Operandi now has a number of contracts for the DCGS computer network that forms the heart of the drone system, notably with the Army and the Marines. [173]

Palantir

Easily the best known company in this field, Palantir of California was created with funding from In-Q-Tel, the investment arm of the CIA.[174] Like Modus Operandi, Palantir sells database visualization products under brand names like Gotham and Raptor to the Pentagon and to industry.

One of Palantir's first customers was the Joint Improvised Explosive Device Defeat Organization (JIEDDO) which bought a license to the Palantir software package to track down planters of

roadside bombs in Iraq. Soldiers fell in love with the visually stunning reports that replaced the legacy spreadsheets with its rows and columns that soldiers had to search one at a time.

"It's like plugging into the Matrix," an anonymous Special Forces member stationed in Afghanistan told *Bloomberg*. "The first time I saw it, I was like, 'Holy crap. Holy crap. Holy crap.' "[175]

"It supports the cops on the streets and the officers doing the investigations. They can now exactly see great information and the links between events and people," Sgt. Peter Jackson of the Los Angeles Police Department was quoted in a company document. "Detectives love the type of information it provides. They can now do things that we could not do before."[176]

Not everybody agrees. Many critics say that while Palantir software can create dazzling displays, it isn't magic. Indeed, internal company documents leaked to *BuzzFeed* suggest that a number of big clients including American Express, Coca-Cola, and Nasdaq have canceled contracts for Palantir visualization software.

For example, in January 2015, after Palantir's software failed to yield results, Coca-Cola backed out of a five-year project to create a data-sharing consortium between consumer packaged goods companies. American Express canceled a contract after 18 months. "We struggled from day 1 to make Palantir a sticky product for users and generate wins," a Palantir employee said of the American Express contract. And Michele Buck, the North American president of Hershey's, said she "did not see value from Palantir." [177]

What does set Palantir apart is an aggressive and unusual marketing strategy. The company regularly gives away software to cultivate well-known clients like the International Consortium of Investigative Journalists. [178] In addition it has also sued the Army to try to force the Pentagon to buy its software and replace the existing DCGS. [179]

Leidos Wisdom and Halogen

Leidos, which is based in Reston, Virginia, offers two data mining products: Halogen and Wisdom. Both products were originally developed by Lockheed Martin. [180] (Lockheed also offers Dragon Dome, a full suite of intelligence tools for aircraft, drones, and satellites as well as GeoLAMP, which manages video and radar data from airborne sensors.) [181]

Wisdom, according to Lockheed's original promotional literature, is "a predictive analytics and big data technology tool that monitors and analyzes rapidly changing open-source intelligence data." Halogen provides security-cleared staff analysts to help compile reports that identify and analyze "human networks and their key components, to include leaders, facilitators, and influencers, as well as the threats and opportunities created by them." [182]

Clients who have bought Wisdom include Walmart, which hired Lockheed to monitor the social media accounts of union activists with Organization United for Respect at Walmart (OUR Walmart) and to track protests planned for Walmart's June 2013 week-long annual meeting in Bentonville, Arkansas.[183]

"With some assistance from LM [Lockheed Martin] we have created the attached map to track the caravan movements and approximate participants," Kris Russell, a Lockheed risk program

SOFTWARE

Mike,
With some assistance from LM, we have created the attached map to track the caravan movements and approximate participants. We may tweak the formatting/cosmetics a little but, this should be pretty much what we stick with through next week. Take a look and let me know what you think or if you have any questions. Thanks!
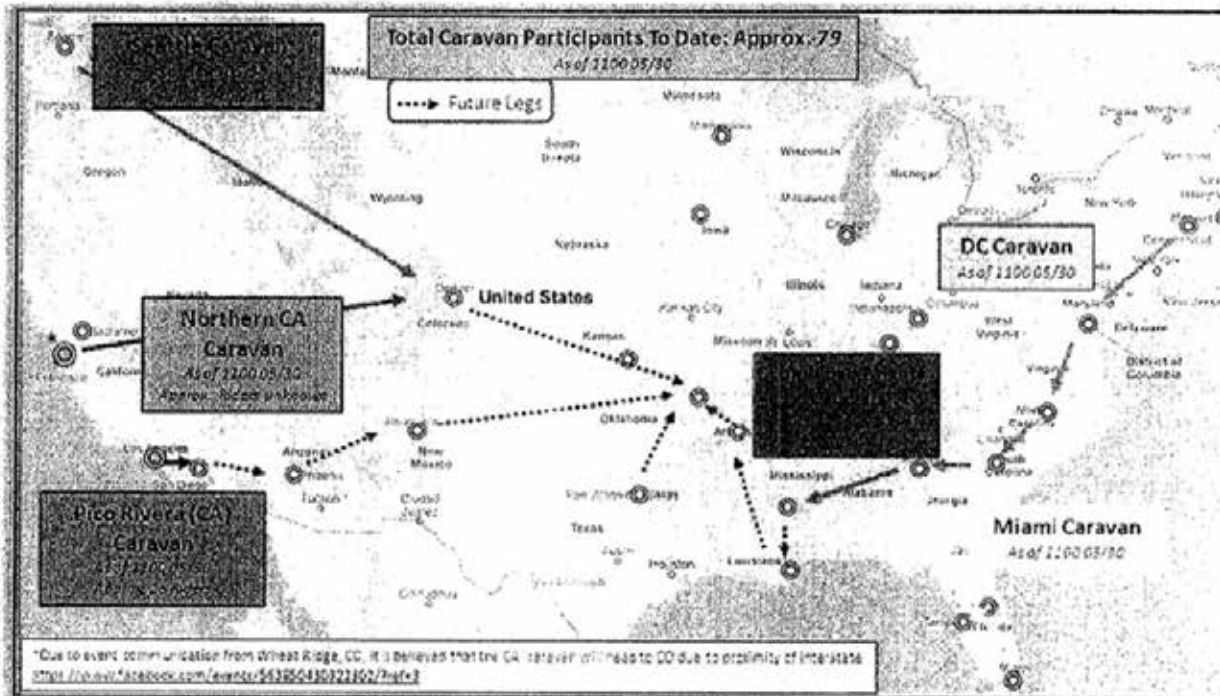
Slide presented in OUR Walmart v Walmart National Labor Relations Board hearing.

senior manager, wrote in an internal email that was revealed after activists sued the company for retaliating against employees who took part in protests.

Organizers who read the internal memos later said that Lockheed's analysis was often wrong. Others noted that it was actually quite easy to mislead the surveillance team. "I sent a couple of fake tweets about where we would be or what we were doing," Angela Williamson, an OUR Walmart organizer told *Bloomberg*. "I wonder how people feel about Walmart wasting money by hiring Lockheed Martin to read my tweets. I wouldn't be happy about that if I was a shareholder."

J. Distributed Common Ground System

"Everyone focuses on this little piece of fiberglass flying around called an unmanned aerial vehicle," Lt. Gen. David Deptula, a key architect of the aerial surveillance system, told *Air Force Magazine* in September 2015. "But it's just a host for sensors that provide data to this vast analytic enterprise we call the Distributed Common Ground System, which turns the data into information and hopefully knowledge."[184]

Housed on dozens of networked military computers scattered around the world, DCGS is built and maintained by over 70 contractors including Booz Allen Hamilton of Virginia, L-3 Communications, Lockheed Martin, and Raytheon. [185]

DCGS allows users to access some 700 disparate sources of intelligence information[186] including live video feeds, thermal imagery, radar, and mobile phone tracking data; take advantage of social network analysis tools including Palantir and Modus Operandi to analyze data; and not least, to set up and execute targeting missions via the NCCT.

A 2015 fact sheet produced by the LeMay Center at Alabama's Maxwell Air Force base best explains the system's capabilities: "An example of cross-cueing would be a DCGS signals operator employing sensors aboard a U-2 on the other side of the planet to geolocate a target signal and then cue a geospatial analyst working in the same room to coordinate with a Predator unit

Air Force Distributed Common Ground System work stations. CREDIT: U.S. Air Force.

thousands of miles away to steer its video sensor to observe the source of the signal, and immediately report their findings directly to a supported unit in the area." [187]

In practice, this means a phone signal tracked by a U-2 pilot flying 60,000 feet over Syria could be observed in close to real time by a DCGS analyst in Virginia who could ask a drone pilot in Nevada to zoom a camera on a Predator at 10,000 feet so that an imagery analyst in Florida could take a closer look before calling in a jet to drop a bomb. The Pentagon calls this "reachback" because it allows troops in the field to get immediate support from military personnel at bases located in the U.S.

The first DCGS was set up in 1994 and dispatched to Guantanamo Bay, Cuba, to support U.S. military operations in Haiti. [188] Since then it has evolved into a global system with five main Air Force DGS hubs—in California, Germany, Hawaii, South Korea, and Virginia—and dozens of smaller sites scattered around the U.S. [189] All military services now have their own versions of DCGS (see box) that can receive and redistribute data from airborne aircraft—from the Predators to the U-2s. [190]

The main DCGS sites are vast, window-less warehouses where analysts work in small groups monitoring multi-screen systems on darkened operation floors.[191] Their main task is processing, exploita-tion, and dissemination (PED). Every day the DCGS commanders create a PED tasking order (PTO) to instruct drone operators on the data they would like to collect. [192] As the data flow back to be

archived, they get tagged and analyzed by software as well as by human operators. DCGS also employs linguists who interpret data and intercepted conversations to ensure accurate tagging and analysis and occasionally to support soldiers in the field in near real time. [193]

"We do data conditioning to help analysis. We help with the mundane tasks to make data ready to be analyzed, make it easier to discover and get on the screen," Patrick Biltgen, a senior mission engineer for BAE Systems Intelligence and Security who worked on DCGS, told *Tactical ISR Technology*. [194]

Yet to this day, DCGS is a multi-billion dollar boondoggle. A staggering 54 out of 64 Air Force DCGS users surveyed by the Institute for Defense Analyses in 2015 gave it less-than-the-minimum score for usability.[195] A 2016 Pentagon evaluation unearthed by CorpWatch suggested that the Air Force system was unavailable 67 percent of the time. [196] And a 2012 Pentagon evaluation reported that DCGS-Army has to be rebooted every eight hours. [197]

To understand why the system is such a shambles, it is important to view DCGS in the context of how the military has historically collected data. "The root cause of many of these difficulties is adherence to a centralized Cold War collection management doctrine focused on production [of large quantities of intelligence] rather than goals and objectives," wrote Col. Jason Brown in *Joint Forces Quarterly* in 2014. At the time, Brown worked at the DCGS base in Ramstein, Germany. Today he has overall responsibility for DCGS as commander of the Air Force's 480th ISR Wing. Its motto is *Non Potestis Latere,* Latin for "You Can't Hide." [198]

TOP 20 DCGS CONTRACTORS	
RAYTHEON COMPANY	$937,264,569.29
SWINERTON INCORPORATED	$54,112,998.35
HARRIS CORP	$52,781,609.87
LOCKHEED MARTIN CORP	$34,380,282.71
HF GROUP INC	$26,415,191.00
RAYTHEON COMPANY	$18,971,081.00
NCI INC	$17,551,661.01
NORTHROP GRUMMAN CORP	$16,899,579.00
CACI INTERNATIONAL INC	$15,650,352.46
GENERAL DYNAMICS CORP	$15,385,841.69
DYNAMIC SYSTEMS INC	$15,160,647.82
L-3 COMMUNICATIONS HOLDINGS INC	$14,736,971.05
BALL CORP	$13,460,006.95
APTIMA INC	$12,425,604.00
CREDENCE MANAGEMENT SOLUTIONS LLLC	$11,999,685.00
UTAH STATE UNIVERSITY	$10,201,480.00
SIERRA NEVADA CORP	$9,952,904.93
EYAK CORP	$9,683,009.03
CRITERION SYSTEMS INC	$9,673,114.49
SPECTRUM COMM INC	$9,369,606.40

For example, ever since the late 1950s, the Pentagon has relied on high-flying spy planes like the U-2 together with satellites to provide information on distant enemies. Intelligence was often derived from a series of high-resolution photographs taken from space. The film was delivered to ground analysts who pored over them for details and especially for changes over time to spot troop or weapons movements. A data request could easily take eight days to fulfill.

Even after the advent of video-equipped drones in Yugoslav war in the 1990s, the analysts continued to follow the old

Data analyzed by CorpWatch from Department of Defense prime- and sub-contract databases from FY2009 through FY2016.

Slide from DCGS January 2016 evaluation. CREDIT: Director, Operational Test and Evaluation, Pentagon.

system by converting video feeds into still images that they printed out on paper and examined.[199]

After the 2003 invasion of Iraq, such methods quickly became moot in Iraq. Soldiers on the ground were no longer trying to detect the advance of slow moving bulky tanks. Instead they were up against shadowy networks of quick-moving urban fighters who could plant a roadside bomb at night and then blow it up by remote control hours or even minutes later.

It didn't help that the analysts had no real understanding of what data to request. "For example, analysts would submit GMTI [requests] over cities failing to recognize the … platform's inability to distinguish moving targets in the clutter of an urban environment," Brown adds. "Many leaders and analysts eventually realized that it was not viable to submit formal intelligence requirements and then hope all the pieces would arrive at the right time."[200]

Meanwhile as new data gathering technologies proliferated, the Pentagon simply tasked new recruits to collect it all, regardless of the ultimate goal. "Current hierarchical collection management processes separate the tasks of collectors, exploiters, and analysts into ever-smaller discrete tasks, but in practice their reassembly downstream rarely works as elegantly as doctrine suggests," Brown wrote in another magazine. "This Industrial Age mentality assumes the end goal is 'finished intelligence' produced in centralized factories assembling components created in isolation from one another."[201]

The biggest such intelligence "factory" is the one that Brown now manages at the headquarters of the 480th Wing at Joint Base Langley-Eustis. [202] Hundreds of analysts work side by side at that at that Hampton, Virginia base, in semi-circular pods of six.[203] Around the world, Brown has a total of 6,000 Air Force analysts working for him at the 27 Air Force DCGS sites. Every single day these analysts manage an estimated 20 terabytes of data that they categorize into searchable databases like UNICORN (the acronym for the unified collections operations reporting network.) [204]

At the same Virginia Air Force base, this data is then converted into strike targets by the 363rd ISR Wing[205] under the command of Col. Michael "MiG" Stevenson.[206] "Our analysts go through and sort through all that and do long-term studies and determine trends. So using their data from a year ago to the present day, we come up and determine: here is what the enemy's doing," Stevenson told local reporters on a March 2015 publicity tour of the base. "It's a very detailed, methodical

process to get targets advanced to the point where they are actually struck by aircraft."[207]

But more candid interviews suggest that the analysts, most of whom joined the military straight out of high school and are rarely older than 25, are simply following a rule book blindly. "Many assume that every crew was aware of what not only they were doing and why, but also what the other assets assigned were doing. The reality is that is not the case," Lt. Commander Peter Salvaggio, who was in charge of a piloted Lockheed EP-3 reconnaissance aircraft, told a military researcher back in 2011. "And the sad part is that you typically find out months later at a conference over a cup of coffee during a BS session. Only then do you find out what was really being requested."[208]

Now, the Air Force wants to solve this problem by entrusting more to algorithms. "We have invested in more airmen analysts, but the growth in our force cannot keep up with the growth of raw data," Maj. Gen. Robert Otto, commander of the Air Force ISR Agency, told the journal *Tactical ISR Technology*. "To deal with this we need to develop more advanced, more automated search and analysis tools."[209]

Yet this approach has already failed and is not likely to improve without investing more in the human element. Automated computer search tools in the hands of young soldiers with no knowledge of cultures half way around the world, are

likely to increase the likelihood of errors, rather than reduce them.

In addition to the overwhelming quantity and often useless quality of data gathered—or perhaps precisely because of it—Pentagon evaluators, as far back as March 2010, have consistently given

> **"Many assume that every crew was aware of what not only they were doing and why, but also what the other assets assigned were doing. The reality is that is not the case."**
>
> **—Lt. Commander Peter Salvaggio**

DCGS a failing grade.[210] This pattern began soon after the contractors were asked to upgrade the software to allow intelligence analysts scattered around the world to collaborate via the internet.[211]

Several years later, all indications suggest that Air Force DCGS is still as clunky. "Major system shortfalls included system instability, slow system response times, and an inability to simultaneously receive and exploit full motion video, Global Hawk imagery, and U-2 imagery," J. Michael Gilmore, director of the Pentagon's Operational Test & Evaluation Directorate (DOT&E), wrote in a 2014 memo to Bill LaPlante, assistant secretary of the Air Force for acquisition.[212] Gilmore noted that the Air Force itself had concluded internally that the system was not "operationally effective or operationally suitable."

To get around this, the Air Force had rigged up a scaled-down version with the elements that had been approved. But Gilmore concluded that the modified version did "not provide a joint,
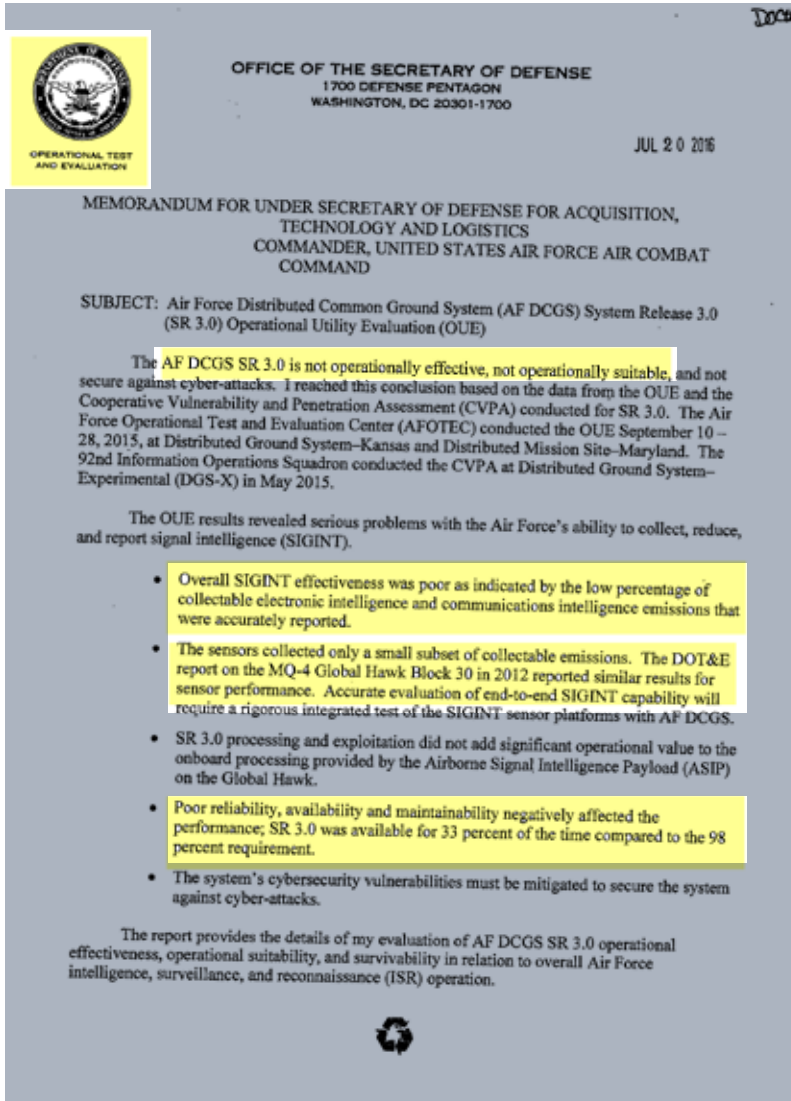
Air Force-Distributed Common Ground System evaluation.

oversight of DCGS into four smaller programs in the hope of getting at least some parts approved. This scheme prompted an angry memo from Gilmore. "The reduced level of oversight and priority is increasing the opportunity for continued problems, lack of resources and priority, and provides a false impression of reduced risk associated with the program," he wrote.[213]

But, instead of consolidating the system, the Air Force then split the oversight of DCGS into eight parts in 2015, which resulted in yet another angry memo from Gilmore. "Such a balkanized test program does not permit an accurate assessment of the overall AF DCGS operational capability," he wrote in a 2016 memo obtained by CorpWatch under the Freedom of Information Act.[214]

In the same memo, Gilmore noted that the AF-DCGS was only up and working 33 percent of the time, despite the contract's requirement for a minimum of 98 percent of the time. "Evaluation results revealed serious problems with the Air Force's ability to collect, reduce, and report signal intelligence."

Meanwhile, the Pentagon's evaluators also reported that the contractors were making little progress with integrating new sensors. By 2016 they had only been able to add one new working element: the synthetic aperture radar system, which is not even widely used.[215]

net-enabled capability for controlling [intelligence] platforms and sharing the data they collect."

To convince evaluators that the system was viable, the Air Force then split the

DCGS-Army

DCGS is not unique to the Air Force. The Army, Marines, Navy and the Special Forces each has its own version of the globally networked computer system, with the Navy even fielding versions on ships. The Army version, built by a number of major military contractors led by Northrop Grumman, has been heavily criticized by soldiers who say that the system barely works, noting that it was even unable to provide routine weather forecasts because of coding errors.[216]

Distributed Common Ground System-Army 2007 handbook cover.

The soldiers have an advocate—Duncan Hunter, a member of Congress from San Diego who has been waging war against the incumbent contractors for years.

"It's supposed to be like this big cloud portal, so that anybody can access it. But nobody does—because it doesn't work! It's like opening PowerPoint or whatever and clicking on everything and nothing works," Hunter told the *New Republic* magazine in 2013. "For all of Afghanistan, it's got a total of sixty-six persons of interest. You would think thousands. It's a complete scam."[217]

Hunter's argument was not welcomed by military top brass, who went as far as to instruct senior officers to push back by calling their own members of Congress.[218] Unfortunately, Hunter undercut his own argument by vehemently supporting a rival system manufactured by Palantir, which has been lobbying to take over the contract.[219]

He revived his criticism in October 2015 when an Air Force AC-130 gunship mistakenly bombed a Doctors Without Borders hospital in the Afghan city of Kunduz, killing at least 22 people and injuring over 30. "My office has learned from multiple service members and officers that … the primary components of the Pentagon's flagship Intelligence system, the Distributed Common Ground System, were not operational in Afghanistan," Hunter wrote in a letter to the Ashton Carter, then head of the Pentagon.[220]

Documents from the DOT&E back up Hunter's criticisms. "Battalion commanders and staff indicated they did not consider [DCGS] to be very helpful for the fight on the ground. As a workaround, some battalion analysts resorted to tracking the battle using pencil and paper," J. Michael Gilmore, the DOT&E director, wrote in a January 2016 evaluation of DCGS-Army.[221]

THE CONTRACTORS

Despite the popular myth that drones are clandestine tools operated by the CIA to kill America's most wanted, the aircraft are really just one element of a vast surveillance system operated mostly by enlisted soldiers. The Air Force takes the lead on flying and managing drones, with support from the other military services and a mix of intelligence agencies.

But rarely acknowledged are the thousands of contractors working alongside government employees to manage the high-tech hardware and software. Laws governing inherently governmental work bar contractors from making targeting decisions or firing missiles, but they do play a critical role in the development, testing, fielding, and maintenance of these technologies as well as in analyzing raw data, for which they are almost never held to account.

As described in previous sections, there are literally dozens of for-profit companies in the drone business from tiny outfits like IISi with six staff to big guns like Lockheed, Raytheon, and Northrop Grumman which employ small armies of people. By far and away, the most important company in this business is General Atomics, which makes the Predator and Reaper, builds the Hellfire missiles, and even provides many of the pilots. But it is likely that companies like L-3 earn just as much from drones, depending on how one categorizes the contracts.

Unfortunately, there is no known official system to track the role of these corporations. But by explaining their specific roles inside and in the context of the military kill chain, we've attempted to chart their scope (see below). Bear in mind that DCGS alone uses some 70 sub-contractors, perhaps many more, so a single chart cannot encompass or explain the extent of the enterprise—even if the information were easily available. Some of the smaller companies are glorified employment bureaus used to provide payroll and other services so commanders can retain soldiers after they finish their service contracts. Then there are even fake companies that the CIA sets up, with no more than a post office box, in order to hide operations from reporters and perhaps even from lawmakers.
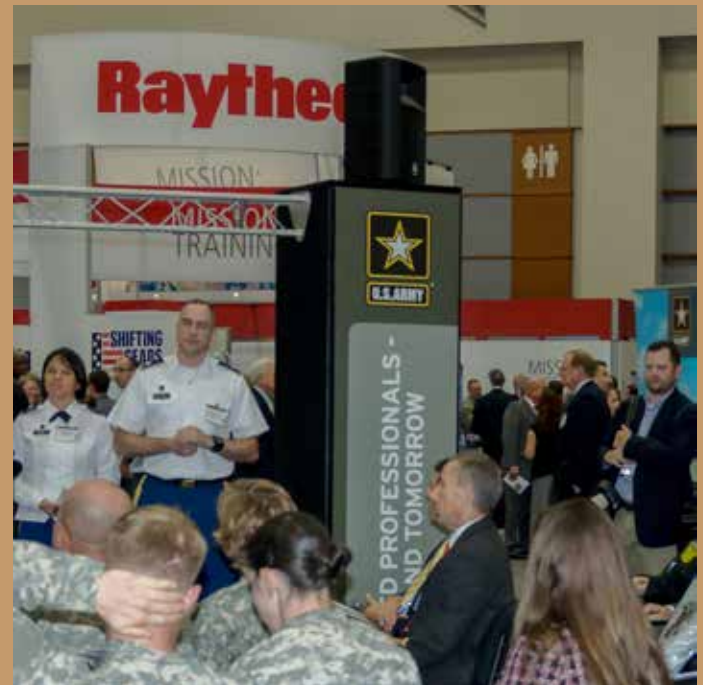
Presentation at Association of the United States Army annual meeting. CREDIT: Tho Le, U.S. Army.

K. Embedded in the Kill Chain

At any given time, the U.S. operates some 60 drone combat air patrols consisting of three to four aircraft. Each individual aircraft—typically Predators and Reapers made by General Atomics—has two sets of assigned pilots (known as 18Xs after their numbered Mission Operation Specialty training) and sensor operators (1U0X1s) who typically work out of ground control stations—identical custom-designed trailers that can be packed up and moved easily from base to base and even overseas. The Air Force uses trailers made by General Atomics. Lockheed and Northrop Grumman also build similar trailers for use with other drones [222]

The pilots are typically officers with college degrees, but the sensor operators—who manage the video cameras, thermal imaging and radar systems—are commonly between 19 and 25 years old, with no more than a high school education. [223] All told a full

Predator crew can have as many as 180 individuals and a Global Hawk can have up to 500. [224]

The first set of pilots, the Launch and Recovery Element (LRE), is usually situated a few hundred miles from the

Combined Air Operations Center, Qatar CREDIT: Alexander Riedel, U.S. Air Force.

KILL CHAIN

Military and Commercial Satellites

NRO Satellite

② Ku-band transmitters on drones and surveillance aircraft relay raw data across the world via satellites.

U-2 Jet 60,000 feet

③ Military pilots use this real time data to fly the drones. Sensor operators and imagery analysts examine pictures. And geolocation analysts use algorithms to try to calculate phone locations.

Drone 10,000 feet

① Mobile phone and radio signals are intercepted by drones, planes and satellites. Individuals are also tracked by video, heat and radar.

④ Guided missiles can be launched from a drone by pushing a button.

Hurlburt Field (Florida) Eustis-Langley (Virginia) Creech (Las Vegas)

AFGHANISTAN

U.S MILITARY BASES

target location.[225] For Pakistan, they may be positioned in the Kandahar or Jalalabad air base in Afghanistan; for Yemen, in Djibouti or Saudi Arabia. LRE pilots are often contractors from companies like Texas-based Aviation Unmanned, General Atomics, and Merlin Ramco of California.[226] Most of them are former Air Force drone pilots, but are paid much higher salaries to work overseas after retirement.

The pilots are accompanied in the field by military and contract radio technicians who manage the satellite data

communications. The main contractor is Northrop Grumman, which operates the Battlefield Airborne Communications Node (BACN) on the ground in countries like Afghanistan, as well as on board piloted aircraft like the Bombardier BD-700. [227]

LRE crews use C-band transmitters to get the drone into cruising altitude close to the target and then hand over control to the second crew known as the Mission Control Element (MCE). [228] One such MCE is the 432nd Air Expeditionary Wing, which manages drones over Ku-band

transmitters, working out of identical Ground Control Stations on the other side of the world at Creech Air Force base in Nevada. [229]

The bigger drones, like Northrop Grumman's Global Hawk, are managed out of Beale Air Force Base in California, as are Lockheed Martin's piloted U-2 aircraft. [230] Other key positions at these U.S.-based sites are the mission intelligence coordinator and safety observer who keep the drones on task and not crashing.

In addition to the global combat air patrols, managed by the Air Force, the Pentagon has employed contractors in Colombia, Iraq, and former Yugoslavia to operate Florida-based AirScan's line-of-sight drones. [231]

The very same surveillance equipment—video cameras, radar and thermal imagers and phone location devices—used on drones is also used on piloted aircraft like Guardrail to complement the drones. [232]

In Africa, U.S. surveillance relies on humble Cessna and Pilatus turbo-prop aircraft that carry similar sensors and transmission equipment as Predators and Reapers. They operate out of covert U.S. bases in Arba Minch, Ethiopia; Camp Lemmonier, Djibouti; Nouakchott, Mauritania; Manda Bay, Kenya; Nzara, South Sudan; and Victoria, Seychelles. Pilots from Sierra Nevada Corporation and R-4 Inc. of New Jersey fly the aircraft. [233] In the Middle East, the U.S. uses custom-designed Boeing 707s and C-135s like the AWACS, JSTARS, and Rivet Joint that

have been conducting surveillance since the 1960s. [234] These aircraft do not carry weapons, but sometimes fly high above drones to help them route their signals to satellites. And then there are the U-2 spy planes that fly at 60,000 feet. [235]

The video footage streaming via satellite from the drones and piloted aircraft is monitored by imagery analysts from both government and the private sector. Government personnel can be located at bases like Beale or Air Force special operations headquarters in Okaloosa, Florida. Contractors come from a variety of companies including 11 listed by the *Bureau of Investigative Journalism*: Advanced Concepts Enterprises, BAE Systems, Booz Allen Hamilton, General Dynamics, Intrepid Solutions, L-3 Communications, MacAulay-Brown, SAIC, Transvoyant, Worldwide Language Resources, and Zel Technologies. [236]

"There are literally dozens of for-profit companies in the drone business from tiny outfits like IISi with six staff to big guns like Lockheed, Raytheon, and Northrop Grumman which employ small armies of people."

Geolocation of phones is also handled by both government and contractors. BAE and Leidos of California run T/F DOA contracts out of Fort Gordon in Augusta, Georgia. [237] Altamira of Virginia also offers Ground Management Target Indicator jobs out of Dayton, Ohio. [238]

Intelligence analysis is performed by the 480th Wing at Joint Base Langley-Eustis in Hampton, Virginia, which manages DCGS. [239] This system integrates

Reaper launch and recovery crew. Kandahar Airfield, Afghanistan CREDIT: Evelyn Chavez, U.S. Air Force.

significant contractor support from the 70-odd contractors like Modus Operandi that work on different aspects of the software. Individual analysts' work is coordinated by regionally themed DCGS Analysis & Reporting Teams (DART) teams using software tools developed by Raytheon and Virginia-based NCI. [240]

The cluttered airspace occupied by drones and piloted planes is managed via the Air Tasking Order (ATO) issued daily by the JFACC (Joint Forces Air Component Commander), while specific data requests are managed via the daily Processing, Exploitation and Dissemination Tasking Order (PTO). [241]

If the drone operation is backed up by soldiers on the ground, it can access Predator feeds from the DCGS via laptop systems like the Remote Optical Video Enhanced Receiver (ROVER) made by L-3 for the Air Force or its Army equivalent, the One System Remote Video Terminal (OSRVT) manufactured by AAI Textron.[242] Soldiers scattered around the world communicate with each other in text-based chat rooms like the multi-user Internet Relay Chat (mIRC). [243]

Coordinating the LRE and MCE with ground forces is a Joint Tactical Attack Controller (JTAC) using L-3's NCCT. [244] When a JTAC wants to conduct a strike, they are expected to fill out a "9-line" order that specifies target location and possible friendly forces, etc. Most strikes involve weeks of planning, unless they involve rapid response for an urgent situation such as troops under fire. [245] In those instances, the JTAC is expected to fill out a DD Form 1972 which is a more complex version of the 9-line. [246] Contractors do not conduct these targeting tasks.

The "floor" Judge Advocate General (JAG) lawyers working out of the Combined Air Operations Center (CAOC) monitor compliance with these rules. [247] For operations in Central Asia and the Middle East, the lawyers often operate out of Al-Udeid air base in Qatar. They are expected to make sure that strikes meet the Laws of Armed Conflict (LOAC), the Rules of Engagement (ROE), and the Special Instructions (SPINS) issued for the particular operation. These legal tasks are also not contracted out. [248]

PTSD

One of the biggest hurdles that the drone war faces is the lack of sufficiently trained pilots and analysts. The Air Force recently announced that it graduates only about 180 drone pilots a year, while some 240 of its 1,260 pilots are not expected to continue after their six-year contracts expire. [249]

When the Government Accountability Office discovered that only about one third of drone pilots had completed their full training before being pressed into service, the Pentagon was forced to cut back on combat air patrols until it could find more properly trained personnel. [250]

In order to fill these positions more quickly, the Pentagon issued a $100 million contract to CAE of Canada to train 1,500 new pilots at Holloman Air Force Base, New Mexico; Creech Air Force Base, Nevada; March Air Reserve Base, California; and Hancock Field Air National Guard Base, New York. [251] Avwatch of Massachusetts also has a contract to do drone simulation training. [252]

Meanwhile, since the military is still very short-handed, it routinely has soldiers pull 12-hour shifts, 6 days a week. As a result, Air Force psychological studies have found widespread stress among pilots, analysts, and operators. "What we see are elevated rates of emotional exhaustion and distress," said Dr. Wayne Chappelle at the School of Aerospace Medicine at Wright-Patterson Air Force Base in Ohio. [253]

Stories of the psychological trauma suffered by lower-ranked Air Force personnel are emerging, including several video documentaries: *Drone* by Tonje Schei, *National Bird* by Sonia Kennebeck and *Unmanned* by Robert Greenwald. [254] Drone personnel—particularly the low-ranked imagery analysts who watch targets day in and day out—testified that the drone war is deeply inaccurate and disturbing.

Brandon Bryant. CREDIT: Brave New Films.

"How many women and children have you seen incinerated by a Hellfire missile? How many men have you seen crawl across a field, trying to make it to the nearest compound for help while bleeding out from severed legs?" Heather Linebaugh, a former drone imagery analyst, wrote in the *Guardian* newspaper. [255] "When you are exposed to it over and over again it becomes like a small video, embedded in your head, forever on repeat, causing psychological pain and suffering that many people will hopefully never experience."

"It was horrifying to know how easy it was. I felt like a coward because I was halfway across the world, and the guy never even knew I was there," Bryant told KNPR radio in Nevada. "I felt like I was haunted by a legion of the dead. My physical health was gone, my mental health was crumbled. I was in so much pain I was ready to eat a bullet myself." [256]

Even DCGS analysts are reporting higher levels of PTSD and several have committed suicide. "My mental, physical and spiritual health are in the dump. Having an inconsistent, unpredictable and work saturated schedule makes opportunities to improve those near impossible to come by," one soldier wrote on a Reddit public web forum on DCGS last year. [257]

Drone, Inc.

TECHNOLOGY/TASK	PRODUCT	COMPANY	HQ
Drone aircraft manufacture	Predator	General Atomics	San Diego, California
	Reaper	General Atomics	San Diego, California
	Global Hawk	Northrop Grumman	Falls Church, Virginia
Missiles	Hellfire	General Atomics	San Diego, California
Piloted aircraft manufacture	AWACS	Boeing	Chicago, Illinois
	Rivet Joint	Boeing	Chicago, Illinois
	Liberty MC-12	Hawker Beechcraft	Wichita, Kansas
	Guard Rail	Hawker Beechcraft	Wichita, Kansas
	EP-3	Lockheed Martin	Bethesda, Maryland
	U-2	Lockheed Martin	Bethesda, Maryland
	JSTARS	Northrop Grumman	Falls Church, Virginia
Line of sight drones		AirScan	Titusville, Florida
Sensor balls & video cameras	Wescam MX series	L-3	New York, New York
	MTS-A & MTS-B	Raytheon	Waltham, Massachusetts
Infra red cameras	Forward Looking Infra Red	FLIR Systems	Wilsonville, Oregon
Synthetic Aperture Radar	Lynx	General Atomics	San Diego, California
	Lynx	Lockheed Martin	Bethesda, Maryland
	TESAR	Northrop Grumman	Falls Church, Virginia
Ground Moving Target Indicator systems	Starlite	Northrop Grumman	Falls Church, Virginia
	VADER	Northrop Grumman	Falls Church, Virginia
		RadiantBlue	Colorado Springs, Colorado
	Kestrel	Sentient Vision Systems	Melbourne, Australia
Phone tracking	T-Pod	BAE Systems	London, UK
	Amberjack	Harris	Melbourne, Florida
	Gossamer	Harris	Melbourne, Florida
	Hailstorm	Harris	Melbourne, Florida
	Harpoon	Harris	Melbourne, Florida
	Stingray	Harris	Melbourne, Florida
	Stingray	Harris	Melbourne, Florida
	Triggerfish	Harris	Melbourne, Florida
	Airhandler	Sierra Nevada	Sierra Nevada
	Gilgamesh	Sierra Nevada	Sierra Nevada
Cross sensor cueing	Network Centric Collaborative Targeting System	L-3	New York, New York
	Cursor-on-Target	Mitre corporation	McLean, Virginia
	Geonet	Ticom Geomatics	Austin, Texas

TECHNOLOGY/TASK	PRODUCT	COMPANY	HQ
Satellite transmission	Ku Band relay	Eutelsat	Paris, France
	Ku Band relay	Inmarsat	London, UK
	Ku Band relay	Intelsat	Luxembourg City, Luxembourg
	Ultra High Frequency MUOS satellites	Lockheed Martin	Bethesda, Maryland
	Ku Band relay	SES	Betzdorf, Luxembourg
Ground control systems	One System Remote Video Terminal (OSRVT)	AAI Textron	Providence, Rhode Island
	Remote Optical Video Enhanced Receiver (ROVER)	L-3	New York, New York
Launch & Recovery of drones	Pilots	Aviation Unmanned	Dallas, Texas
	Pilots	General Atomics	San Diego, California
	Pilots	Merlin Ramco	Solana Beach, California
Piloted aircraft operation	Pilots	R-4	Eatontown, New Jersey
	Pilots	Sierra Nevada	Sparks, Nevada
Data relay from drones	Battlefield Airborne Communications Node	Northrop Grumman	Falls Church, Virginia
Imagery Analysis	Full Motion Video Analysts	Advanced Concepts Enterprises	Shalimar, Florida
	Full Motion Video Analysts	BAE Systems	London, UK
	Full Motion Video Analysts	Booz Allen Hamilton	McLean, Virginia
	Full Motion Video Analysts	General Dynamics	Falls Church, Virginia
	Full Motion Video Analysts	Intrepid Solutions	Sterling, Virginia
	Full Motion Video Analysts	L-3	New York, New York
	Full Motion Video Analysts	MacAulay-Brown	Dayton, Ohio
	Full Motion Video Analysts	SAIC	McLean, Virginia
	Full Motion Video Analysts	Transvoyant	Alexandria, Virginia
	Full Motion Video Analysts	Worldwide Language Resources	Walnut Creek, California
	Full Motion Video Analysts	Zel Technologies	Hampton, Virginia
Phone tracking	Signals Analysts	Altamira	McLean, Virginia
	Signals Analysts	BAE	London, UK
	Netezza GeoSpatial	IBM	Armonk, New York
	Signals Analysts	Leidos	Reston, Virginia
Social Network Analysis	Blade	Modus Operandi	Melbourne, Florida
	Gotham, Raptor	Palantir	Palo Alto, California
	Halogen, Wisdom	Leidos	Reston, Virginia

CONTRACTORS

Drone, Inc.

TECHNOLOGY/TASK	PRODUCT	COMPANY	HQ
Distributed Common Ground System		BAE Systems	London, UK
		Booz Allen Hamilton	McLean, Virginia
		ESRI	Redlands, California
		General Dynamics	Falls Church, Virginia
		L-3	New York, New York
		Leidos	Reston, Virginia
		Lockheed Martin	Bethesda, Maryland
		ManTech	Fairfax, Virginia
		Northrop Grumman	Falls Church, Virginia
		Raytheon	Waltham, Massachusetts
Targeting	Network Centric CollaborativeTargeting System	L-3	New York, New York
Pilot Training	Surrogate Predator program	Avwatch	Plymouth, Massachusetts
	Predator training program	CAE	Montreal, Canada
Testing & Analysis	Next Dollar Sensitivity Tool	Booz Allen Hamilton	McLean, Virginia
	Business Analytics & Optimizationfor Intelligence	IBM	Armonk, New York
	Layered ISR Capabilities Effectiveness Tool	Northrop Grumman	Falls Church, Virginia
	BlueSim	RadiantBlue	Colorado Springs, Colorado
	Operational Test and Evaluation Services	Spectrum	Newport News, Virginia

* This list of companies is not exhaustive. For example DCGS alone has some 70 contractors. The Rivet Joint surveillance system was originally made by Boeing but has been modified by E-Systems, General Dynamics, L-3 Lockheed and LTV at different times in its history.

L. No Bid Deals & Revolving Doors

While many contractors in the drone program are simply hardware and software manufacturers or suppliers of service personnel, others are deeply involved in the development of new technology. These companies, frequently headed by former senior Pentagon executives, are often awarded contracts without having to compete.

Big Safari

Perhaps the key player in this business is 645th Aeronautical Systems Group, a secretive Air Force technology contracting program. Nicknamed Big Safari, it operates out of the Wright-Patterson base in Dayton, Ohio. [258]

Created during the Cold War to help the United States spy on the Soviet bloc, Big Safari claims that it has the legal authority to bypass most military bureaucracy including competitive bidding requirements. The first project

Big Safari logo.

Air Force presentation at Association for Unmanned Vehicle Systems International Unmanned Systems convention. CREDIT: Michael Carden, U.S. Army.

TOP 20 ASC/WI CONTRACTORS: 2008-2017	
L-3 COMMUNICATIONS HOLDINGS INC	$7,576,127,302.37
TELEDYNE TECHNOLOGIES INC	$4,505,213,028.73
GENERAL ATOMIC TECHNOLOGIES CORP	$3,774,153,277.42
SIERRA NEVADA CORP	$2,996,837,809.31
NORTHROP GRUMMAN CORP	$1,125,126,977.65
RAYTHEON COMPANY	$1,029,893,101.80
NORTHROP GRUMMAN CORP	$1,022,633,928.00
ATI LADISH MACHINING INC	$786,930,863.50
BAE SYSTEMS PLC	$758,880,153.58
UNITED TECHNOLOGIES CORP	$380,793,587.08
HAWKER BEECHCRAFT INC	$315,239,088.39
LOCKHEED MARTIN CORP	$262,438,425.73
RIVERSIDE RESEARCH INSTITUTE	$145,210,189.32
SPIRAL SOLUTIONS & TECHNOLOGIES INC	$143,979,013.41
MAV6 LLC	$114,872,280.79
WIEDEMANN CONSULTING	$82,557,333.95
FORCEX INC	$78,774,697.01
VIASAT INC	$78,281,825.02
RAVE COMPUTER ASSOCIATION INC	$74,291,855.00
AURORA FLIGHT SCIENCES CORP	$70,662,317.00
SAIC/LEIDOS HOLDINGS INC	$56,911,272.47

Data analyzed from Aeronautical Systems Center, Intelligence Surveillance and Reconnaissance/Special Operations Forces Directorate, parent office of Big Safari.

the group managed was the so-called Boston Camera. With a 240-inch focal-length lens, the three-ton camera was hidden inside a cargo aircraft named Pie Face. Built in 1952 to be flown over East Germany and operated for ten years, the camera was plagued with vibration problems and the images it shot were often covered with smears. [259]

Beginning in 2001, Big Safari brought together Raytheon and General Atomics to put a sensor system on the Predator (as described in the introduction). [260] Over the last 16 years, Big Safari has been busy handing out new drone development contracts. "We work some of the departments' most sensitive projects and they are all along the lines of intelligence, surveillance and reconnaissance operations," Col. Edward Topps, commander of the group between 2010 and 2014, told *Vocativ* website.[261]

Between 2005 and 2012, Big Safari awarded $31 billion in contracts, *Vocativ* calculated, and estimated that some 96 percent of the money was awarded without competition. [262] One of the big winners was Nevada-based Sierra Nevada Corporation, which was given $3.5 billion in contracts over a seven-year period. In addition to manufacturing Airhandler and Gilgamesh phone-location devices and managing piloted surveillance programs in Africa, Sierra Nevada was also paid to develop the Gorgon Stare program—a nine-camera array designed, not unlike the Boston Camera, to photograph an entire city. [263]

"By dispensing with what its leaders disdained as 'administrivia' and working hand-in-glove with defense contractors and the operators of its aircraft … Big Safari could get innovative gear into action within months, weeks and sometimes even days," writes Richard Whittle in *Predator.* [264]

But six decades after Big Safari put the first giant eye into the skies, critics are still complaining about the quality of the imagery produced by these massive surveillance systems, according to a draft audit of the project uncovered by Winslow Wheeler, then-director of the Straus Military Reform Project at the Center for Defense Information. [265]

Big Safari is able to run legal rings around the Pentagon's own bureaucracy via Quick Reaction Capabilities (QRC), a mechanism intended for emergency situations as an alternative to the normal "Program of Record" system. Many QRCs, like Boston Camera and Gorgon Stare, fail initial testing just as quickly as they were set up.

Other branches of the military also use QRCs and experiment with new drone technology, for example, the Navy's Division 312— the Electronics, Sensors and Networks arm of the Office of Naval Research (ONR), headquartered in Arlington, Virginia. Supporting ONR, is the office of Small Business Innovation Research (SBIR) that has funded projects like Ticom Geomatics Dragonfly, and ISRNet (described earlier). [266]

PEO IEW&S

The Army equivalent of Big Safari is the Program Executive Office for Intelligence, Electronic Warfare & Sensors (PEO IEW&S) at Aberdeen Proving Ground in Maryland [267] and it, too, has a less-than-stellar record in producing intelligence gathering technology. The office memorably spent $902 million over nine years to develop the Ground Based Common Sensor Program. GBCS was envisaged as a radio listening station that could be parachuted into war zones and assembled in less than eight minutes. First commissioned to E-Systems, a division of Raytheon, and then to Loral, a division of Lockheed, GBCS was finally canceled in 1999 after a series of scathing audits. [268]

"The Ground Based Common Sensor Program was not managed efficiently and effectively," a July 26, 1999 report

from the Pentagon's Inspector General charged. "The GBCS System was not able to reliably receive, record, or determine the direction of conventional or low-probability-of-intercept signals. Test results, also, indicated that the GBCS System was not rapidly deployable or highly mobile." [269]

The Pentagon replaced the GBCS with the Prophet, an imposing "all weather, near-real-time, ground-based, tactical signals intelligence/electronic warfare" armored vehicle that could be driven anywhere to listen for enemy chatter. [270] But that seems to have fared little better. Shane Harris, author of *@War*, summed up the program in 2004 simply: "Military intelligence units ... were using the Prophet not to collect signals but to transport food and other material around the base." [271]

Part of the problem was that by the time the physically imposing Prophet was ready to be driven around cities (where it stuck out like a sore thumb), nobody was still using push-to-talk radios. The entire world, civilians and insurgents alike, were communicating with mobile phones and the internet, signals that the Prophet was not designed to intercept.

Task Force Odin patch.
CREDIT: Public domain,
Wikipedia.

Task Force ODIN

In Norse mythology, Odin is the one-eyed god of war and death who leads a noisy band of slain warriors across the sky. Legend has it that he left his other eye in the well of wisdom so that he could see and know everything.

In August 2006, Army Gen. Richard Cody created an unmanned aviation battalion that adopted the Norse name as an acronym for Task Force Observe, Detect, Identify, and Neutralize (TF ODIN) as a field component to PEO IEW&S.

To this day, the ODIN battalion has big dreams for the future. "Big Safari offers a single program office for cradle-to-grave management of the Air Force's QRC special projects. It is [the Program Manager of Observe, Detect, Identify]'s long term vision to become the Army´s Big Safari," wrote Lt. Col. Moises Gutierrez, commander of the program in 2012. [272]

Strip away the military jargon, and what the Observe, Detect, Identify office wants is the opportunity to conduct real-world experiments with new drone technology in the battle field without the usual bureaucracy and oversight.

But an assessment of ODIN's experiments depends on how one evaluates its accomplishments.

In the early years of the war in Iraq, ODIN used Warrior Alpha drones, also manufactured by General Atomics, to track down weapons suppliers in Iraq. Such programs are very hard to assess, but a cache of documents released by Wikileaks in 2011, did shed light on at least one: Operation Seventh Veil. [273]

"The idea [behind] Seventh Veil is … to understand weapons trafficking systems. It allowed us to understand who were the key players within the networks that were operating in our area of responsibility that we needed to go after. And it gave us legitimate cause to go after some of these players," Col. JB Burton, who took part in a 2007 operations, told the Institute for the Study of War. [274]

In September 2009, Operation Seventh Veil was used to track alleged weapons smugglers purportedly entering the country from Syria. Yet, half of the 22 reports filed after two months of careful surveillance sum up their experiences as "ineffective." The others do not evaluate the surveillance operations, but not one weapons smuggler was arrested as a result of the operation. [275]

On September 5, the military requested that F-16 jets be deployed under Operation Seventh Veil to perform "close air support" to monitor eight individuals crossing the border. When the planes swooped down for a better look, they were very disappointed. "At approximately 0220, CAS also identified large flocks of sheep in the vicinity of the individuals. We assess the individuals are shepherds and were moving their flocks," the log records. [276]

Pretty soon, the Warrior Alpha drone picked up some more individuals, who were unloading boxes from a group of donkeys. The Airborne Infantry was dispatched to help the local Iraqi police arrest the individuals. "425 LRS arrive on scene and identify the items as cartons of cigarettes … no foreigners found. … This was a cigarette-smuggling attempt into Syria." [277]

Not one of the 22 missions found any guns. One of the final reports, filed on October 26, 2009, gave some details on the smugglers. "Brawler along with IBP (Iraqi Border Police) located 8x boxes of cigarettes and detained 1x LN (Local National)… from Rummah. He said he has been smuggling for 10 years to support his family, earning 20USD per delivery, he says he never caries [sic] a weapon." [278]

ODIN has claimed more success in tracking down bomb planters, however. In 2006, the unit claimed it had used drones and ground troops in Iraq to kill 2,400 bomb-planters and capture 141. [279] The number of roadside bombs plunged, suggesting success. But by 2009, the numbers were back up again. [280]

Program managers say they had second thoughts later. "'Kill' isn't the only answer here. This is a counterinsurgency fight,"

Lt. Col. Kevin Diermeier of ODIN told *Wired* magazine. "You can't just say, 'I captured this dude, I killed this dude, I'm making a difference,' Maj. Jason Periatt added. "I go back to the '80s. We started rolling up drug dealers. That doesn't mean you're necessarily [succeeding]." [281]

Revolving Doors

The Big Safari procurement program appears to have paid off well for Col. Edward Topps and Lt. Col. Kevin "Ducky" Hoffmann, the two men in charge of developing armed and networked drones in 2001.

Hoffman, who was program manager for the MTS-A and the Hellfire missile on the Predator and the Reaper, left the Air Force in 2010 to join Intuitive, a Huntsville, Alabama company where his new title was "director of Air Force Programs." [282]

In May 2014, Topps retired from running Big Safari for the Air Force. Ten short months later he took up a new job with none less than Sierra Nevada Corporation, one of Big Safari's top grantees. He is now vice president for programs, according to his own online resume. [283]

In 2015, Intuitive and Sierra Nevada joined forces to bid on an Air Force contract to build JSTARS surveillance planes. [284]

CONCLUSION
The Failure of Remote Control War

"America does not take strikes to punish individuals; we act against terrorists who pose a continuing and imminent threat to the American people. Before any strike is taken, there must be near-certainty that no civilians will be killed or injured — the highest standard we can set."

President Barack Obama, May 23, 2013[285]

"It takes a network to defeat a network."

John Arquilla and David Ronfeldt, RAND Corporation[286]

Drones are an integral part of the massive new technology-driven intelligence, surveillance, and reconnaissance system that is slowly transforming the way the U.S. goes to war. Commanders believe that this system of "network-centric warfare," *i.e.*, the network of sensors, aircraft, computers, and analysts provides them with a precise way to find and eliminate alleged terrorists hiding in plain sight within the civilian population.

The methodology that the military follows is known as F3EAD: Find, Fix, Finish, Exploit, Analyze, and Disseminate. [287]

Find. The military tries to analyze electronic communications en masse. Its primary techniques are social network analysis and pattern-of-life analysis. The names and mobile phone serial numbers of potential targets are then added to special watch lists.

Fix. Drone sensors are programmed to log the activity of all mobile phones and radios within range and check to see if any of the devices from the watch lists have been turned on. If any are detected, the camera of the nearest drone can be automatically pointed on that area.

Finish. Troops are sent to capture or kill the target. If a "positive-ID" can be made, and the risk to civilians is minimal, drones can be authorized to fire missiles when troops cannot be deployed.

The latter three steps: **Exploit, Analyze,** and **Disseminate** involve the collection of data from targets under surveillance after capture/kill operations to find leads for more targets, and finally, create new lists of new targets.

The first problem with this "network-centric war" is that the hardware sensors often don't work properly, as we have shown. The image quality is not good enough to determine the gender of the targets, let alone their identities. Thermal imagery sensors often miss entire people. The location data from these sensors is often missing altogether, making it hard to archive and search imagery. Phone numbers for targets are not always accurate. Inherent errors in calculating the location of the surveillance drones themselves throw off their ability to triangulate targets below. Thus even under the best circumstances, target geolocation data can be off by several meters.

The drone war is also heavily dependent on computer databases that contain hundreds of thousands of entries from arrests, informant tips, and biometric data gathered in numerous ways. Yet such databases are routinely inaccurate: In March 2017, a report Government Accountability Office report to Congress found that roughly 15 percent of U.S. citizens whose identities are stored in the FBI's U.S. facial recognition database were flat out wrongly identified and that black people were subject to even higher misidentification rates.[288] The same inaccuracy holds for the notorious no-fly lists, which even contain Congress members and military veterans.[289] It is hardly likely that a database of Afghan or Yemeni citizens would be more accurate.

JUAS-COE
Training Document
Organic/Non Organic UAS
Creech AFB, NV

EMPLOYMENT OF GROUP 3/4/5 ORGANIC/NON ORGANIC UAS TACTICAL POCKET GUIDE

ARMY

MQ-1B PREDATOR
MQ-1 WARRIOR A
MQ-1C ER/MP
MQ-9 REAPER
MQ-5B HUNTER
RQ-7B SHADOW

FEBRUARY 2010
FOR OFFICAL USE ONLY (FOUO)

Table 2. Sensor Matrix	
Advantages	**Disadvantages**
Electro-Optical	
Affords a familiar view of a scene.	Employment of camouflage and concealment techniques can deceive the sensor.
Offers system resolution unachievable in other optical systems or in thermal images and radars.	Restricted by weather conditions; visible light cannot penetrate clouds or fog.
Preferred for detailed analysis and measurement.	Restricted by terrain and vegetation.
Can provide 3 D imaging for better analysis	Limited to lighted areas during nighttime.
Infrared	
A passive sensor, impossible to jam.	Not as effective during thermal crossover (1 to 1.5 hours after sunrise or sunset).
Offers camouflage penetration.	Tactical platforms threatened by threat air defenses.
Provides good resolution. Night imaging capability.	Bad weather degrades quality.
Synthetic Aperture Radar	
Near continuous SA even in adverse weather	No video capability. Not supported by OSRVT.
Detailed imaging of large area	Extensive processing and distribution bandwidth
Photographic-like images	Image latency based on resolution
Ground Moving Target Indicator	
Provides increased UA survivability through increased stand-off ranges	Additional processing may be required. Will miss stationary targets

Drone operator's manual, Creech Air Force base.

Next, there is the problem of faulty algorithms and software. Using radar to find a ship on a wide-open ocean is easy, as is detecting an intruder at a gate. Yet to this day, determining the precise location of a mobile phone, or even spotting tanks on the ground from the air, remain challenging. Given that cameras can easily be auto-cued to watch the wrong phone, it is no wonder that so many individuals have been reported "killed" multiple times, and that the bodies of children are regularly found in the debris after a drone strike.

The military often refers to the surveillance system, including drones, as the "Unblinking Eye." But if DCGS, the heart of this system, is unavailable two-thirds of the time and when most users don't understand how to use the complex, unwieldy beast, the number

of cameras in the sky makes little difference.

Using mathematical models like Greedy Fragile to identify and destroy a network also won't work. Pattern recognition from electronic data is deeply problematic, especially on a foreign culture with tribal networks that stretch back for centuries. It is also easy to confuse a politician with an insurgent or a weapons smuggler with a cigarette smuggler. Even hitting the "right" target might actually make a network more dangerous if it caused an insurgency to splinter or more cruel leaders to take control. Several studies conducted by Rex Rivolo of the Institute for Defense Analysis, the Pentagon's think tank, have shown these outcomes in Afghanistan and Colombia. Rivolo quoted a U.S. soldier he met in Iraq who told him: "Once you knock them off, a day later you have a new guy who's smarter, younger, more aggressive and is out for revenge."[290]

Finally, the skillset of those hired to watch these so-called dark networks virtually guarantees confirmation bias: The majority—enlisted soldiers, straight out of high school—have no cultural tools to assess the data they gather; the
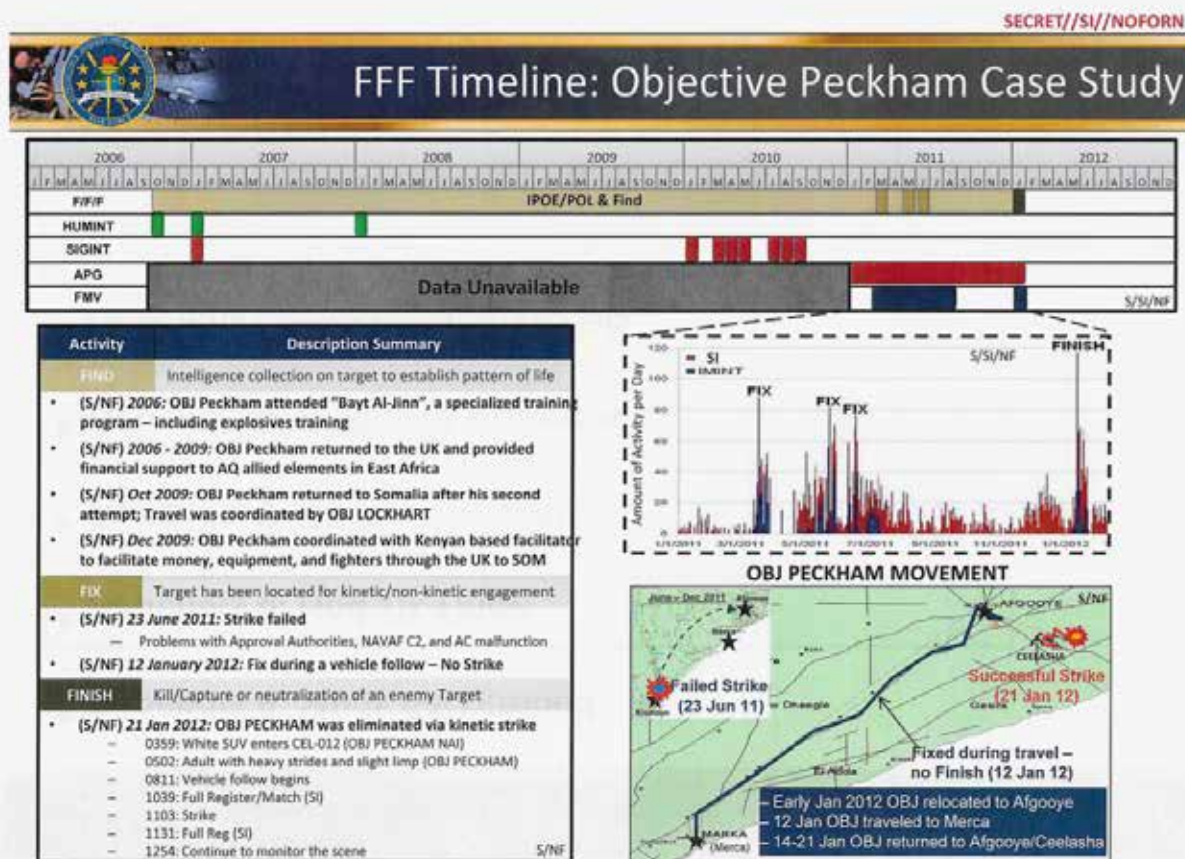
FFF Timeline: Objective Peckham Case Study

for-profit contractors rely for their jobs and salaries on producing intelligence, even if it is less than adequate.

Can the technology be improved and is that, in any case, really the right question? The biggest hurdle in the drone war isn't better cameras or a more aircraft or faster data transmission. Those might be solved with money and time. A much bigger problem is a lack of understanding of the assumptions behind the algorithms used to seek out targets, and a failure to honestly assess the quality of the raw data and auto-cueing systems.

Technology Cannot Replace Human Intelligence

Despite these problems, the drone/surveillance program has many supporters who cite examples like JIEDDO which combined drone video with mobile phone network data to track down the individuals planting bombs on Iraqi roads to target U.S. vehicles. The program worked very well, but it had a crucial component that the drones in Pakistan and Yemen do not: Soldiers who could meet with tribal leaders, kick down doors, and interrogate people.

As Lt. Col. John Nagl, a retired Army battalion commander who helped write the new military counterinsurgency field manual, asked *Wired* magazine: "The police captain playing both sides, the sheikh skimming money from a construction project, what color are they?" referring skeptically to the color-coded targets on a computer map. [291]

Some battalion commanders are very much aware that no matter how much data they get from them, drones have their limits. "The enemy will be located not by satellites and UAVs (unmanned aerial vehicles), but by patient intelligence work, back alley payoffs, collected information from captured documents, and threats of one-way vacations to Cuba," Maj. Gen. Robert Scales, former commandant of the U.S. Army War College, told a U.S. congressional hearing. "If I know where the enemy is, I can kill it. My problem is [that] I can't connect with the local population." [292]

Without a presence on the ground, sensor-led intelligence is dangerous. The argument that poor video can be fixed with good phone locations falls apart given that phone numbers are often swapped around. The big problem is confirmation bias, which cross-sensor cueing exacerbates, as does cursor-on-target systems. As the cliché goes, if you only have a hammer, everything looks like a nail.

Even drone contractors admit the problem with systems like DCGS. "You cannot automate analysis; that is judgment—it would be like automating a

Lt. Col. John Nagl. CREDIT: Gerry Gilmore, American Forces Press Service.

Maj. Gen. Paul Van Riper.
CREDIT: U.S. Marine Corps.

U.S. soldiers, fighting from the other side of the world, never come to physical harm. Finally, there is also no doubt that a laser-guided missile launched from a Predator or Hellfire can easily target and kill a specific person or destroy a specific building, if their location is established beyond the shadow of a doubt.

Despite these limitations, when commanders observe suspected insurgents through a screen, they place far more faith in the ability of the technology inside the machine to discern truth and to make life or death decisions, far more than they would in an individual human.

"They want to apply the technology without the brainpower. The difficulty is that those who put forth this argument believe that something fundamentally has changed, and you can change very quickly without thinking your way through it," Lt. Gen. Paul Van Riper, former president of the Marine Corps University told *PBS*. "Nothing has happened that's going to change the fundamental elements of war."[294]

Auditing the Drone Program

There are very few publicly available audits of the overall effectiveness of drones, given their clandestine use. One of the only detailed assessments is an eight-year-long investigation of Predator surveillance of the U.S.-Mexico border (referenced earlier) conducted by the inspector general of the Department of Homeland Security (DHS). It recommended that, given the low rate of detection of border crossers by drones, the government would be much better off investing in alternatives such as manned aircraft and ground surveillance.

jury," Patrick Biltgen of BAE told *Military Geospatial Technology* magazine. [293]

As journalists, we know only too well how hunches are often wrong and need to be carefully double-checked. Then there is the problem of red herrings, laid deliberately to frame certain individuals or to inflame tensions. None of these difficulties can be overcome by peering from two miles up through a virtual soda straw.

That is not to say that drones don't work at all. While they cannot replace on-the-ground research, drones can, first, clearly provide quite good overwatch for soldiers in the field. Second, drones can be used to gather raw data for future analysis in remote areas to which the military has no quick or easy access. Third, the drone program ensures that

"We see no evidence that the drones contribute to a more secure border, and there is no reason to invest additional taxpayer funds at this time," Inspector General John Roth concluded in a January 2015 press statement.[295]

Pressed for an explanation as to why the program had failed to meet its own goals, DHS continued to insist that the drones had been worth the money. "We are working on metrics which have never been done before," Randolph Alles, assistant commissioner in charge of the Office of Air and Marine, told a July 2015 hearing of the Homeland Security Subcommittee on Border and Maritime Security. "How do you characterize air support? How do you characterize the effectiveness of an aircraft for surveillance? How do you put a dollar value on it?"[296]

Yet Homeland Security had set out crystal clear goals when starting up the program in 2004: increased apprehensions of illegal border crossers, a reduction in border surveillance costs, and improvement in the Border Patrol's efficiency. None of these goals were met.

Could the same be true of the targeted killing program? On the face of it, one might assume that the two programs have different goals. Yet, border drones, with only one simple task—identify people crossing a clearly defined border—failed miserably. How then could the same sensors on the very same aircraft identify terrorist plots and plotters across an entire region?

A 2012 audit of Air Force surveillance programs by the House Permanent Select Committee on Intelligence complained that the military was measuring the success its systems in much the same way as Homeland Security.[297]

Instead of measuring how many high-value targets are caught, the Pentagon "tends to measure outputs, *e.g.,* how long can a platform stay on station, what is the resolution of the sensor's imagery, or even how many requests were made for a given sensor's data and anecdotal evidence about what is useful or not in theater," the auditors wrote.

And then there is the problem of the size of the data haystack the drones are producing. Publicly released studies suggest that the deluge of data they collect has not proven very useful, if only because there is too much flowing back to the analysts.

"The rapid proliferation of sensors both enables and overwhelms the current ISR infrastructure," concluded the Defense Science Board in its 2008 study. "The number of images and signal intercepts are well beyond the capacity of the existing analyst community so there are huge backlogs for translators and image interpreters and much of the collected data are never reviewed." [298]

Even when reviewed, the data can be just wrong. Several official studies have clearly shown that drones make major mistakes because of bad data. Dr. Larry Lewis, formerly with the Center for Naval Analyses, conducted a study of civilian casualty incidents in Afghanistan, where ground troops conducted battle damage assessments following airstrikes. He identified civilians killed or wounded in 21 cases. Yet in 19 of those 21 cases, preliminary evaluations conducted via drone video cameras had identified no civilian casualties. Though his study remains classified, Lewis has spoken out about his findings.

"The fact that I had been looking at air operations in Afghanistan for a number

Maj. Gen. James Poss.
CREDIT: U.S. Air Force.

of years led me to suspect that what I found was in fact the case," Lewis told the *Guardian* newspaper.[299]

In 2015, *The Intercept* published details from several other studies leaked by a whistleblower. One showed that during a five-month period in eastern Afghanistan, more than nine out of every 10 people killed in U.S. drone strikes weren't the intended targets.[300]

In his investigation into the Uruzgan strike that killed 23 innocent villagers including women and children, Maj. Gen. James Poss concluded: "Technology can occasionally give you a false sense of security that you can see everything, that you can hear everything, that you know everything." [301] Vicki Divoli, former deputy legal advisor to

the CIA's Counterterrorism Center, was even more succinct: "Intelligence is not evidence."[302]

But one doesn't even have to investigate the killing program in Pakistan and Yemen to show that drones can't accurately find people. *New York Times* reporter David Rohde can personally testify to this. He was kidnapped near Kabul and imprisoned for seven months in Waziristan before he escaped in June 2009.

"My family said U.S. officials had told them that they searched exhaustively for me with drones, but had been unable to locate me," Rohde wrote in *The Atlantic* magazine. "When I met U.S. officials, they told me that they had not known I was being held prisoner in the house close to [a] drone strike in Makeen."[303]

Warren Weinstein and Giovanni Lo Porto were not as lucky. Like Rohde, they were never located by the U.S. even after three years in captivity in the Pakistan borderlands patrolled by drones. In January 2015, the two hostages were killed when drone commanders signed off on a strike after surveillance data indicated that that no civilians were present.

So why use drones? "The drone's unique characteristic — that it is piloted from the ground not the air — cloaks it in a technology that seems to intrigue policy makers. It gives them a self-perceived license to employ the system over ambiguous or hostile territory such as Pakistan, and Iran," Winslow Wheeler of the Center for Defense Information in Washington, wrote in *Time* magazine after reviewing studies from DOT&E. "The wide and enthusiastic popularity for … drones, in the Defense Department, the Executive branch, Congress, the mainstream media and think tanks is not

rationally explained by Reaper's poor to mediocre performance."[304]

Indeed, Wheeler notes that drones are typically twice as expensive to build as piloted aircraft and four times as expensive to maintain because of the enormous numbers of ground personnel required to support them. (The studies also found that drones are more vulnerable to attack and to crash—topics that are beyond the scope of this report.)

There do appear to be some internal (and likely classified) measurements of the effectiveness of drone surveillance. At least four contractors—Booz Allen, IBM, Northrop Grumman and RadiantBlue—claim to have developed tools for this precise purpose, mostly to identify cost savings, but also to aid in planning.[305]

Phil Eichensehr of RadiantBlue told congressional staff that their BlueSim product was being used by the Joint Staff to "model technical performance of ISR platforms and sensors." Frank Strickland of IBM claimed that its tool could be used to "evaluate the

effectiveness of each platform and sensor for counterinsurgency."

A set of leaked slides from IBM analyses, published by *The Intercept*, provides further proof that these tools have been used internally. One of these slides provided a tantalizing, if obscure, clue: a statistical breakdown of what tracking technologies were used to locate drone targets.[306] While the numbers them-

"Technology can occasionally give you a false sense of security that you can see everything, that you can hear everything, that you know everything."

— Maj. Gen. James Poss

selves don't mean much, the existence of the slides suggests that the Pentagon has kept track of the use of surveillance technology and has even provided it to outside analysts. Such data should also be provided to independent human rights observers. Such contractor-driven studies may not be as critical as one might hope, but there are several other government mechanisms by which the targeted killing system can be held to account. That is the subject of our final chapter.

NEXT STEPS

Political leaders insist that the drone war's combination of multiple layers of hardware and software has allowed the military to win wars without putting boots on the ground. Soldiers, for their part, place a high degree of trust that these technologies will find the right targets from halfway across the world. However, well-hidden engineering errors embedded in this vast and complex intelligence enterprise have given both politicians and the military a false confidence.

Perhaps the greatest problem is confirmation bias—because one flawed technology simply exacerbates the errors of other flawed technologies. A full evaluation of these technologies is long overdue.

A few brave whistleblowers in the Air Force, notably low-ranked imagery analysts and sensor operators who watch targets day in and day out, have stepped forward to say that the tools simply don't work. Their testimony complements and corroborates the numerous reports from local media on the ground in targeted communities as well as investigations by respected international human rights groups.

Meanwhile contractors are profiting from the lack of proper oversight and controls on selling hardware and software that has never been properly tested.

We believe that the time is ripe for military commanders and members of the U.S. Congress to seize the initiative to review the last decade of targeted killing and demand a rigorous system of checks and balances.

There are multiple existing mechanisms that can be used to review these flawed drone technologies and contractors: The Government Accountability Office, the Congressional Research Service, and the armed services and intelligence committees in Congress can each do its part. Less well-known but equally important entities like the Defense Contract Audit Agency and the inspectors general of each agency have the ability to raise critical questions.

And there are other, perhaps less obvious, ways to tackle these problems. For example, every day military lawyers, judge advocate generals, on the "kill floor" have an opportunity to question the data that strike commanders present to them. They can examine the quality of the video and phone location data as well as question the algorithms by which targets are tracked. Commanders can support whistleblowers by taking their complaints seriously and protecting them against retaliation. Even at the battalion level, commanders have the ability to request independent reviews whenever there is an allegation of error or misconduct such as the killing of innocent people.

In reality, the most effective check on the drone war to date has been the Pentagon's Operational Test & Evaluation Directorate. This unlikely and obscure office has acted as brake on Big Safari and PEO IEW&S, where contractors have had a field day selling poor and sometimes downright faulty technology.

DOT&E

Most modern military systems, including drone aircraft, take many years to develop. The Pentagon buys such new technologies via a system of incremental testing known as the "evolutionary acquisition program."[307] First it publishes a wish list of the "increments" or components it would like the new system to include, and then it invites companies to compete for the contract to build trial versions of each item for testing.

When any stand-alone element passes the required tests and is considered "operationally effective, suitable, and survivable" the military puts in a big order. That's not the end of the process though since the wish list typically grows. The contractors go away and design new capabilities, which the Pentagon then subjects to yet more tests. Over time, sometimes even decades, the Pentagon allows the "acquisition" of a full system to "evolve," resulting in quicker delivery and allowing for mid-course corrections of errors in specific components.

The job of DOT&E is to conduct independent testing of these experimental military systems at every stage of this evolutionary cycle. Not only does the agency have the power to field test each component of a new system, it can force contractors to go back to the drawing board and fix major flaws before placing a big order.

The first set of DOT&E tests for a new system is called the Initial Operational Test & Evaluation (IOT&E); the second is the Follow-on Operational Test & Evaluation (FOT&E). Technologies are typically ranked on "key performance parameters."[308] Quite often a system that has been judged operationally

effective, suitable, and survivable for military purchase may still have minor or even fairly serious flaws or shortcomings that DOT&E has recommend be fixed. The final IOT&E and FOT&E reports can thus be a gold mine of details of possible problems for commanders, policy makers and journalists.

After DOT&E tests each part of the system, the Pentagon continues to request updates via a confusing system of "blocks." Thus, the first version of the Reaper drone was Block 1 and the second was Block 5. [309] But the first Global Hawk drone was Block 10, followed by Block 20, Block 30, and so on.[310] The F-35 fighter started out with Block 1A, followed by Block 1B, then Block 2A, Block 2B, Block 3i and Block 3F. [311]

Components of the drone system put through this DOT&E evaluation system include the sensors, the database systems, and the aircraft themselves. But as we have shown in the case of

Director, Operational Test and Evaluation logo.

Big Safari's request that many drone technologies be approved via the Quick Reaction Capabilities cycle, the Pentagon's normal methodical approach has often been circumvented.

Given the opportunity, DOT&E has produced many critical reports on the drone system. Here is a list of a few such audits:

Predator: The Predator, manufactured by General Atomics, was not initially designed to fire weapons or track signals, but rather to broadcast near real-time video. It can stay aloft for 24 hours and fly 770 miles without refueling. More than seven years after its first flight in 1994, Big Safari chose the Predator to be modified for surveillance and war fighting after the September 11 attacks. Both the MTS-A sensor ball and the Hellfire missile, designed for helicopters, were adapted for the Predator in the experiments described in the introduction. [312]

DOT&E was not impressed with the first results of the jury-rigged drone. In October 2001, the agency concluded that the Predator was "not operationally effective or suitable."[313] "[P]oor target location accuracy, ineffective communications and limits imposed by relatively benign weather, including rain" were just some of the problems afflicting the Predator.

Data from a series of DOT&E tests in Nevada showed that when the Predator was flying at 30,000 feet, the infrared cameras were able to detect only 21 percent of wheeled vehicles and identify the vehicles correctly just five percent of the time. [314]

Reaper: The Reaper drone, also manufactured by General Atomics, first flew

in May 2001. It has a range of 1,150 miles and can spend 30 hours in the air. In 2009 DOT&E rated the Reaper as effective in the "killer" role, but said it was not able to verify the effectiveness of the "hunter" role, notably because the synthetic aperture radar system was not working. [315]

Global Hawk: The Global Hawk program was first launched in 1998. Manufacturer Northrop Grumman boasts that the plane can survey "vast geographic regions with pinpoint accuracy … in all types of weather—day or night." It is designed to fly almost 14,000 miles without refueling and stay aloft for 34 hours. [316]

However, the drone has spent much of the last two decades on the ground since it is not able to fly through storms or icy weather. A May 2011 DOT&E report concluded that the Global Hawk was only functional about 40 percent of the time and did not recommend using it during a crisis or war. [317]

The report noted that the drone suffers from "frequent failures of mission-critical air vehicle components reduce takeoff reliability and increase mission abort rates." An Air Force officer, interviewed by Andrew Cockburn, explained this problem in more descriptive terms: "Junk is right. It's made of composite plastic with adhesives instead of nuts and bolts to keep the weight down but that glue doesn't work so well so internal parts, fuel lines and electrical conduits, come apart in flight."[318]

Cockburn's source also says that the Global Hawk sensors are terrible. "The infrared can pick out campfires but that's about it, and that's only when it's directly over the target, and you need the target's cooperation for that. The radar

Predator wreckage, Djibouti, May 17, 2011. CREDIT: U.S. Air Force.

suffers from the plastic airframe twisting and flexing at high altitude so the picture shifts with it."

The DOT&E report also calculated that the Global Hawk was only able to find the "signal source geographic locations" in seven out of 10,719 signals, *i.e.,* less than one-half of one percent of detected signals. [319]

Gorgon Stare: A nine-camera array designed to be carried by drone to conduct "wide-area persistent surveillance," Gorgon Stare was built by Sierra Nevada with funding from Big Safari. On its launch in January 2011, it was championed by Maj. Gen. James Poss, Air Force assistant deputy chief of staff for intelligence, surveillance and reconnaissance. "Gorgon Stare will be looking at a whole city, so there will be no way for the adversary to know what we're looking at, and we can see everything," he told the *Washington Post.*[320]

Just three weeks later, a leaked DOT&E report revealed that the Gorgon Stare cameras were "marginally sufficient to track vehicles [but] not sufficient to track [people]. "In general, [infrared] imagery quality is poor, which yields marginal mission capability at night." Large area pictures are "subject to gaps between stitching areas, which manifests itself as a large black triangle moving throughout the image." Three months later, in April 2011, Poss admitted that poor quality Predator drone video imagery had led soldiers to kill 23 unarmed villagers in Uruzgan. [321]

CorpWatch believes that the DOT&E reports should pro-actively release all completed evaluations. Failing that, we urge advocates and the media request these reports under the provisions of the Freedom of Information Act. Many reports are nominally public, but aren't easy to find since the agency only publishes a summary report each year with conclusions from the latest tests and projects dates for upcoming tests.

In collaboration with the National Security Archive in Washington DC, CorpWatch has requested a number of existing evaluations and we hope to make them available in coming months once they have been reviewed by Pentagon lawyers and released to us.

Key Federal Oversight Agencies

Congressional Research Service (CRS): This research agency provides nonpartisan, objective policy and legal analysis to the U.S. Congress. CRS has issued overview reports on the use of drones by the Pentagon as well as the potential for domestic drone use. [322]

Defense Contract Audit Agency (DCAA): The Pentagon's audit agency conducts 76 percent of all civilian agency audits and 89 percent of all federal contracting audits. The agency maintains offices on the premises of Lockheed Martin, Raytheon, and Northrop Grumman and has the authority to examine secret contracts via its Field Detachment division. [323]

Government Accountability Office (GAO): The audit arm of the U.S. Congress the GAO has broad powers to investigate how the federal government spends money. It has issued critical reports on drone pilot training and on DCGS. [324]

Inspectors General (OIGs): Most federal agencies have an independent office charged with investigating criminal activity as well as waste, fraud, and abuse within their parent agency. The Department of Homeland Security Office of Inspector General issued an excellent report on the failure of drones on the U.S.-Mexico border, while the Pentagon's Inspector General has critically reviewed the Gray Eagle, Hunter, and Reaper drone programs. [325]

Judge Advocate Generals (JAGs): Military commanders have the authority to appoint officers to conduct an investigation into misconduct, accidents, and criminal activities. The Army investigation is an AR 15-6; the Air Force's is a Commander Directed Investigation (CDI). [326] The commander who authorizes the report also has the authority to release it to the public. The AR 15-6 investigation into the February 2010 killing of 23 villagers in Uruzgan was notable for making public the live chats among drone personnel. [327]

Whistleblowers

Chris Aaron: (CIA and National Geospatial Intelligence Agency, 2006-2009)

Chris Aaron. CREDIT: Chris Aaron

"When you're really drinking the government Kool-Aid, it's very easy to get caught up in the group think. [But] we were playing the game of Whack-A-Mole. How many of those people did we kill? [Yet] the next day, there were all these new targets. I began to see a real lack of foresight."[328]

"There was absolutely a lot of guess work involved, a lack of coordination. We lacked a central database. Can you imagine it? To keep all of our targets organized. [Meanwhile] there was constant turnover amongst [drone operators] in the war, you had new people coming in every few weeks, every few months. Sometimes there was only 24 hours continuity between people. So if there was one person who was an expert on a target, when the new person comes in, suddenly all that information is gone. So [when] someone new [arrived], for all they know there's a bunch of chickens running around as opposed to a bunch of children."[329]

Chris Antal: (Army chaplain, 2008-2016)

"Democracy is about due process. These drone wars have blown due process up in smoke. They've blown checks and balances up in smoke."[330]

"We have sanitized killing and condoned extrajudicial assassinations: death by remote control, war made easy without due process, protecting ourselves from the human cost of war."[331]

"The reason why I became a shareholder [of Honeywell] is because I was frustrated with the lack of progress through legislative advocacy, and I believe what

Chris Antal. CREDIT: Bob Fernandez, Philadelphia Inquirer.

we are facing in our country is not just a military-industrial complex, that Eisenhower wrote about, it's a military-industrial-congressional complex."[332]

Brandon Bryant: (Air Force sensor operator, 2006-2011)

Brandon Bryant: "I killed 13 people with a total of five Hellfire missile shots, and only three of them were actual combatants."

Amy Goodman (interviewer): "Who were the others?"

Brandon Bryant: "We don't know. I don't know. I would like to know."[333]

"This figure runs around the corner, the outside, toward the front of the building. And it looked like a little kid to me. Like a little human person. There's this giant flash, and all of a sudden there's no person there. [I] asked, "Did that look like a child to you?" They typed a chat message to their screener, an intelligence observer who was watching the shot from 'somewhere in the world'—maybe Bagram, maybe the Pentagon. And he says, 'Per the review, it's a dog.'"[334]

"Combat is combat. Killing is killing. This isn't a video game. How many of you have killed a group of people, watched as their bodies are picked up, watched the funeral, then killed them too?"[335]

Michael Haas: (Air Force sensor operator), 2005 to 2011)

"Ever step on ants and never give it another thought? That's what you are made to think of the targets—as just black blobs on a screen. You start to do these psychological gymnastics to make it easier to do what you have to do—they deserved it, they chose their side. You had to kill part of your conscience to keep doing your job every day—and ignore those voices telling you this wasn't right."[336]

"It was a pretty fucked up time. There was a lot of coke, speed, and that sort of thing. Everyone drank. We used to call alcohol drone fuel because it kept the program going. If the higher ups knew, then they didn't say anything, but I'm pretty sure they must have known. It was everywhere."[337]

Stephen Lewis: (Air Force sensor operator, 2005 to 2010)

Stephen Lewis, Kathleen McClellan, Cian Westmoreland, Jesselyn Radack, Michael Haas, Brandon Bryant. (left to right) CREDIT: Johannes Berg.

Stephen Lewis: "It was late 2009, and I was tasked to go support a troop in contact. It was four guys walking down a mountain path. And I didn't see any weapons. I didn't see anything. We were given clearance to fire the missile. About five minutes goes by, and two Hellfires come in and they kill three people. And there was one wounded guy left. And that guy just—he just wasn't there anymore."

Juan González (interviewer): "This is—you were given clearance to fire at the wounded guy on the ground."

Stephen Lewis: "Yes." [338]

"You're creating an atmosphere of fear. And there's an old saying in Texas: You don't back a scared animal up against the wall. And if you do that, he's going to come out fighting. And that's exactly, I think, what's happening now." [339]

Heather Linebaugh: (Air Force imagery analyst, 2009-2012)

Heather Linebaugh.CREDIT: Ten Forward films.

"The U.S. and British militaries insist that this is an expert program, but it's curious that they feel the need to deliver faulty information, few or no statistics about civilian deaths, and twisted technology reports on the capabilities of our UAVs." [340]

"Hearing politicians speak about drones being precision weapons [makes it seem like they're] able to make surgical strikes. To me it's completely ridiculous, completely ludicrous to make these statements." [341]

"We always wonder if we killed the right people, if we endangered the wrong people, if we destroyed an innocent civilian's life all because of a bad image or angle." [342]

"When you are exposed to it over and over again it becomes like a small video, embedded in your head, forever on repeat, causing psychological pain and suffering that many people will hopefully never experience." [343]

Lisa Ling: (Air Force DCGS operator, 2007-2012)

"There's a bomb. They drop it. It explodes. Then what? Does somebody go down and ask for somebody's driver's license? Excuse me sir, can I have your driver's license , see who you

are? Does that happen? I mean, how do we know? How is it possible to know who ends up living or dying?" [344]

Lisa Ling. CREDIT: Ten Forward films.

"I just want people to know that not everybody is a freaking terrorist, and we need to just get out of that mindset. And we just need to see these people as people—families, communities, brothers, mothers, and sisters, because that's who they are. Imagine if this was happening to us. Imagine if our children were walking outside of the door, and it was a sunny day and they were afraid because they didn't know if today was the day that something would fall out of the sky and kill someone close to them. How would we feel?" [345]

"We are participating in a war overseas. And we have no connection to it other than wires and keyboards. Because if that's the only connection, why stop?" [346]

Cian Westmoreland: (Air Force radio technician, 2006-2010)

"Within the system, the responsibility for killing the person is divided, so nobody feels the full responsibility of what they're doing. And I think that we're moving towards a world where—in aerial warfare, where increasingly there's going to be more technicians and less decision makers." [347]

"Every time we kill a civilian, it creates hatred in the families. If they don't have anywhere else to turn, they are going to turn to radical organizations." [348]

Daniel X: (Signals Intelligence Analyst, dates not revealed)

"[Drones] just embolden commanders, they embolden decision makers. Because there is no threat [to U.S. soldiers], there is no immediate consequence." [349]

Daniel X. CREDIT: Ten Forward films.

"When we are in our darkest places and we have a lot to worry about and we feel guilty about our past actions. It's really tough to describe what that's like. Having the image in your head of taking your own life is not a good feeling." [350]

Drone, Inc.

(Endnotes)

1   Eli Watkins, "US strikes Yemen more in a few weeks than it did all last year," CNN, April 4, 2017.
2   "Yemen 2017 Drone Strikes," The Bureau of Investigative Journalism, June 16, 2017.
3   "United States Policy on Pre – and Post-Strike Measures to Address Civilian Casualties in U.S. Operations Involving the Use of Force," White House Executive Order, July 1, 2016.
4   "Drone Warfare," The Bureau of Investigative Journalism.
5   Human Rights Watch, "Between a Drone and a Al-Qaeda: The Civilian Cost of US Targeted Killing in Yemen," Human Rights Watch, October 22, 2013. See also: "Will I be next?" U.S. Drone Strikes in Pakistan," Amnesty International, October 2013.
6   Spencer Ackerman, "US drone strikes more deadly to Afghan civilians than manned aircraft – adviser," The Guardian July 2, 2013.
7   "US Drone Strikes Kill 28 Unknown People for Every Intended Target, New Reprieve Report Reveals," Reprieve press release, November 25, 2014.
8   "Summary of U.S. Counterterrorism Strikes Outside Areas of Active Hostilities between January 20, 2009 and December 31, 2015," Office of the Director of National Intelligence press release, July 1, 2016.
9   Richard Whittle, "Predator: The Secret Origins of the Drone Revolution," Henry Holt, 2014.
10   Christopher Nerney, "UAV Flies Prototype Signals Intelligence System," Space Tracks, October 2001.
11   "ASPO deploys Tactical Exploitation System to Navy Fleet Battle Experiment – India," The Eagle, October 2001.
12   Whittle, op. cit.
13   Spencer Ackerman, "Air Force Is Through With Predator Drones,"Wired, December 14, 2010.
14   Alexander Orlov, "The U-2 Program: A Russian Officer Remembers," Center for the Study of Intelligence, Central Intelligence Agency, April 14, 2007.
15   "U-2 Dragon Lady factsheet," Lockheed Martin website, undated. Accessed June 13, 2017.
16   "MC-12 factsheet," Air Force website, posted January 21, 2016.
17   "E-8C Joint Stars factsheet," Air Force website, posted September 23, 2015.
18   "RC-135V/W Rivet Joint factsheet," Air Force website, posted May 23, 2012.
19   Craig Whitlock, "U.S. Expands Secret Intelligence Operations in Africa," Washington Post, June 13, 2012.
20   Christina Clausen, "Flying the RPA Mission," 432nd Air Expeditionary Wing Public Affairs, March 22, 2016.
21   W.J. Hennigan, "Air Force hires civilian drone pilots for combat patrols; critics question legality," Los Angeles Times, November 15, 2015.
22   Dianna Cahn, "Intelligence Airman at Langley Keep an Eye on War," Pilot Online, March 21, 2015.
23   David Zucchino and David Cloud, "U.S. deaths in drone strike due to miscommunication report says," Los Angeles Times, October 14, 2011.
24   William Booth, "More Predator drones fly U.S.-Mexico border," Washington Post, December 21, 2011.
25   Heather Linebaugh, "I worked on the US drone program. The public should know what really goes on," The Guardian, December 29, 2013.
26   Rafiuddin Mehsud, "The lost culture of South Waziristan Agency, Fata," Pakistan Daily Times, May 24, 2011.
27   Linebaugh, op. cit.
28   Andrew Cockburn, "Kill Chain: Drones and the Rise of High-Tech Assassins," Verso Books, 2015.
29   Jon Leachtenauer and Ronald Driggers, "Surveillance and Reconnaissance Systems: Modeling and Performance Prediction," Artech House Optoelectronics Library, 2001.
30   Ibid.
31   "MTS-B Sensors Help 'Grim Reaper' Harvest Enemy Targets," Defense Industry Daily, January 24, 2010.
     WESCAM in $200M deal for targeting system," Defense News July 20, 2010.
32   "National Image Interpretability Rating Scales," Posted on the website of the Federation of American Scientists, January 16, 1998.
     "Standard Video-National Imagery Interpretability Rating Scale," Posted on the website of the Geospatial Intelligence Standards Working Group on February 27, 2014.
33   Ibid.
     See also Erik Blasch & Bart Kahler, "Application of VNIIRS for Target Tracking," May 2015.
34   Bruce Bennett, Dillon Bussert and Daniel Goldstein. "Analysis of Operational Airborne ISR Full Motion Video Metadata," Military Communications Conference, San Diego, CA, November 18-20, 2013.
35   Ibid.
36   Mike Tully, "Just How Accurate is Your Drone?," Aerial Services Inc., January 20, 2016.
37   Patrick Coffman, "Capabilities assessment and employment recommendations for Full Motion Video Optical Navigation Exploitation," Naval Postgraduate School, Monterey, June 2015.
38   David Cloud, "Anatomy of an Afghan war tragedy," Los Angeles Times, April 10, 2011.
39   Ibid.
40   "Pakistan Reported U.S. Strikes 2015," The Bureau of Investigative Journalism, May 1, 2015.
41   "Statement by the President on the Deaths of Warren Weinstein and Giovanni Lo Porto," White House press release, April 23, 2015.
42   Greg Jaffe, Adam Goldman and Greg Miller, "Officials fear CIA missed opportunity to identify Western hostage," Washington Post, September 10, 2015.
43   Adam Entous, "Obama Kept Looser Rules for Drones in Pakistan," The Wall Street Journal, April 26, 2015.
44   Leachtenauer and Driggers, op. cit.
45   "Airborne Systems factsheet," FLIR Military & Defense website, undated. Accessed June 13, 2017.
46   "Technical Note: Seeing Through Fog and Rain with a Thermal Imaging Camera," FLIR Military & Defense website," undated. Accessed June 13, 2017.
     See also Van Hodgkin and Ronald Driggers, "3rd Generation Thermal Imager Sensor Performance," U.S. Army Night Vision and Electronic Sensors Directorate, November 1, 2006.
47   Mark McCurley. "I was a Drone Warrior for 11 Years. I Regret Nothing," Politico, 2015.
48   Lisa Parks, "Drones, Infared Imagery, and Body Heat," International Journal of Communication, 2014.
49   Zucchino and Cloud, op. cit.
50   "Transcript of U.S. Drone Attack," Los Angeles Times, April 8, 2011.
51   "Sandia, General Atomics unveil new fine resolution synthetic-aperture radar system," Sandia press release, August 28, 1999.
52   Christian Wolff, "Synthetic Aperture Radar Tutorial," undated. Accessed June 13, 2017.
53   "Predator RQ-1 factsheet," Air Force Technology website, undated. Accessed June 13, 2017.
54   N. Milisavljevic, D. Closson and I. Bloch, "Detecting Human-Induced Scene Changes Using Coherent Change Detection in SAR Images," International Society for Photogrammetry and Remote Sensing technical symposium, July 2010.
55   Robert Ackerman, "Strike Fighters Partners with Pilot," Signal, October 2006.
56   Gregory Newstadta, Edmund Zelnio, LeRoy Gorham and Alfred Hero, "Detection/Tracking of moving targets with synthetic aperture radars," Air Force Research Laboratory, April 18, 2010.
57   Armin Doerry, "Motion Measurement for Synthetic Aperture Radar," Sandia National Laboratories, January 2015.
58   Margaret Cheney and Brett Borden, "Problems in synthetic-aperture radar imaging," Naval Postgraduate School, 6 August 2009.
59   "NASA Evaluates Compact Synthetic Aperture Radar," NASA press release, November 27, 2001.
60   Douglas Starr. "What Your Cell Phone Can't Tell the Police," New Yorker, June 26, 2014.
61   Interview with Michael Cherry, April 2017.
62   Fabian van den Broek, "IMSI Catching," Institute for Computing and Information Sciences, Radboud University, June 23, 2016.
63   Mark Godsey, "Cell Tower Triangulation – How it Works," The Wrongful Convictions Blog, June 1, 2012.
64   John Kelly and Brendan Keefe, "911's Deadly Flaw: Lack of Location Data," USA Today, February 22, 2015.
65   Jeremy Scahill and Glenn Greenwald, "The NSA's Secret Role in the U.S. Assassination Program," The Intercept, February 9, 2014.
66   Bruce Schneier, "Everything we Know About How the NSA Tracks People's Physical Location," The Atlantic, February 11, 2014.
67   "Bureau Hid Doubts About Reliability of Stingray Evidence Behind Redaction Marks," The Intercept, January 31, 2017.
68   "Airhandler PGL Payloads on UAVs factsheet," Document posted on The Intercept.
     "Gilgamesh PGL Payloads on UAVs factsheet," Document posted on The Intercept
69   "Traveler Pod – T-Pod PGL Payloads on UAVs factsheet," Document posted on The Intercept.
70   Stingray Tracking Devices factsheet," American Civil Liberties Union, undated. Accessed June 13, 2017.
71   Ryan Gallagher, "Meet the Machines that Steal Your Phone's Data," ArsTechnica September 25, 2013; Lorenzo Franceschi-Bicchierai, "Here's a Picture of a Phone-Tracking Device that We've Never Seen in the Wild," Motherboard November 22, 2016.
72   "What is GPS? factsheet" Garmin website, undated. Accessed June 13, 2017.
73   Fred Zahradnik, "Assisted GPS, A-GPS, AGPS," Lifewire, June 7, 2017.
74   Spencer Ackermann and Noah Shachtmann, "Almost 1 In 3 U.S. Warplanes Is a Robot," Wired, January 9, 2012.
75   Clausen, op. cit.
     Nick Turse, "The Stealth Expansion of a Secret U.S. Drone Base in Africa," The Intercept, October 21, 2015.
76   "Predator RQ-1 factsheet," Air Force Technology. op. cit.
77   Clausen, op. cit.
78   Kristan Campbell, "11th ATKS Paves Way with Training," 432nd Air Expeditionary Wing Public Affairs public affairs, March 29, 2017.
     Mark Mazzetti, "The Drone Zone," New York Times, July 6, 2012.
79   "Intelsat General's Broadband Solutions for Government Airborne Applications facsheet," Intelsat General Corporation February 14, 2014.
     Stephen Long, "Challenges in Achieving Optimum FMV Capabilities,"
     Northrop Grumman powerpoint, November 2011.
80   Andy Beegan, "SATCOM for ISR factsheet," Harris website, undated. Accessed June 13, 2017.
     Craig Covault, "UAVs Drive SATCOM Modernization," Defense Media Network October 26, 2010.
81   Chris Foresman, "US Broadband's Average Speed: 3.9Mbps," Arstechnica, January 18, 2010.
82   "Award Reflects the Flexibility of the Intelsat Fleet," Intelsat press release, March 24, 2009.
     "SES Charts Rising Government Needs," SES White Paper, SES, November 2016.
83   William Graham, "ULA Atlas V Successfully Launches with MOUS-5 for the US Navy," NASA Spaceflight.com, June 23, 2016.
84   "Bringing Home the BACN to Front-Line Forces," Defense Industry Daily, June 16, 2015.
85   Stew Magnuson,"Military 'Swimming in Sensors and Drowning in Data,'" National Defense magazine, January 2010.
86   "Report of the Joint Defense Science Board Intelligence Science Board Task Force on Integrating Sensor-Collected Intelligence," Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, November 2008.
87   Frank Pasquale, "Digital Star Chamber," AEON, August 18, 2015.
88   Leonard A. McGee and Stanley F. Schmidt. "Discovery of the Kalman Filter as a Practical Tool for Aerospace and Industry," NASA technical memorandum #86847, November 1985.
89   Yaakov Bar-Shaalom faculty profile, University of Connecticut website. Accessed June 13, 2017
     Henk Blom faculty profile, University Delft website. Accessed June 13, 2017.
90   "SKYNET: Courier Detection via Machine Learning," The Intercept June 6, 2012.
91   Martin Robbins, "Has a rampaging AI algorithm really killed thousands in Pakistan?" The Guardian, February 18, 2016.
92   Noah Shachtman, "Death by Algorithm: West Point Code Shows Which Terrorists Should Disappear First," Wired, December 6, 2012.
93   Mike Strasser, "Counter IED Software developed this summer at West Point," West Point public affairs, 2014.
94   David A. Mindell, "Automation's Finest Hour: Radar and Systems Integration in World War II," Systems, Experts and Computers, Massachusetts Institute of Technology Press, 2003.
95   "Radar: Factors Affecting Radar Performance," Encyclopædia Britannica , undated. Accessed June 13, 2017.
96   Mark O'Hair, Bradley Purvis and Jeff Brown, "Aided versus automatic target recognition," Proceedings of the SPIE, Volume 3069, 1997.
97   James Ratches, "Review Of Current Aided/Automatic Target Acquisition Technology For Military Target Acquisition Tasks," Optical Engineering, July 2011.
98   Patrick Miller, "UAV Sensor Sensibility," UAS magazine, April 18 2016.
99   "U.S. Custom's and Border Protection's Unmanned Aircraft System Program Does Not Achieve Intended Results or Recognize All Costs of Operations," Office of Inspector General, Department of Homeland Security, December 24, 2014.
100 Henry Canaday, "Automatic Intelligence," Tactical ISR Technology, August 5, 2013.
101 Radiant Blue membership listing in Geospatial Intelligence Forum magazine, May/June 2010.
102 Kimberly Hale, "Expanding the Use of Time/Frequency Difference of Arrival Geolocation in the Department of Defense," Rand Institute, September 2012.
103 Ibid.
104 Ibid.
105 John Pike, "Guardrail Common Sensor," Federation of American Scientists February 22, 2000.
     Brandon Pollachek, " Guardrail Turns 40, Modernization Keeps it Going," US Army July 7, 2011.

106 Frank Calvelli, Statement to the Subcommittee on Strategic Forces, Committee on Armed Services, U.S. House of Representatives, March 15, 2016.
107 Ryan Gallagher, "Inside Menwith Hill," The Intercept, September 6, 2016.
108 Hale, op. cit.
109 Volkan Tas, "Optimal Use of TDOA Geo-Location Techniques Within the Mountainous Terrain of Turkey," Naval Postgraduate School, September 2012.
110 Suzanna Koster, "Haqqani is not our Problem, Pakistan Says," Global Post, September 30, 2011.
111 Netezza V. Intelligent Integration Systems, Civil Action No. 09-4961-BLS, Suffolk Superior Court, Massachusetts.
112 Netezza V. Intelligent Integration Systems, Motion for Summary Judgment, IISI Slide #105.
113 Deposition of Jon Shepherd in Netezza V. Intelligent Integration Systems, April 6, 2010.
114 "Netezza Spatial: Bringing High-Performance Location Intelligence into the Data Warehouse" Product brochure submitted as document # NZA000180 in Netezza V. Intelligent Integration Systems.
115 Deposition of James Baum in Netezza V.Intelligent Integration Systems, April 15, 2010.
116 Email of Skip McCormack dated October 14, 2009, submitted as document # NZA0010590 in Netezza V. Intelligent Integration Systems
117 "Netezza Performance Server System Delivers 20x Performance Increase and Helps the DNC "Get Out The Vote," Intelligent Integration Systems Incorporated press release, November 9, 2006.
Presentation of Paul Davis to Boston Entrepeneurs Forum, September 6, 2011
118 Affidavit of Richard Zimmerman in Netezza V. Intelligent Integration Systems, September 8, 2010
119 Deposition of Richard Zimmerman in Netezza V. Intelligent Integration Systems, April 12, 2010
120 IISI Slide #139 & #140, op. cit.
121 IISI Slide #129, op. cit.
122 IISI Slide #133, op. cit.
123 Statement of relevant facts in support of motion for preliminary injunction, in Netezza V. Intelligent Integration Systems, submitted September 7, 2010.
124 Affidavit of Matthew Kadillak, September 13, 2010, in Netezza V.Intelligent Integration Systems.
125 IISI Slide #154 & #157, op. cit.
126 IISI Slide #163, op. cit.
127 Ritsuko Ando, "IBM to buy analytics company Netezza for $1.7 billion," Reuters, September 20, 2010.
128 "Air Force Research Laboratory's Sensors Directorate fact sheet," Wright-Patterson Air Force base website, undated. Accessed June 13, 2017.
129 Chris Pocock, "L-3 ComCept has Made Data Fusion a Reality," AIN Online November 30, 2006.
130 "ISR Networking, Analytics & Processing, Exploitation, and Dissemination Solutions fact sheet," L-3 website, undated. Accessed June 13, 2017.
131 Chuck Paone, "Hanscom to host Cursor on Target users meeting next week, 66th Air Base Wing Public Affairs, September 16, 2009.
132 Tricia Bailey, "Cursor on Target: The "Sum of All Wisdom" Comes of Age," MITRE, December 2010.
133 Henneberger v. Ticom Geomatics, Inc. et al, 3:16-cv-00138
134 "U.S. Trade Mark Registration Number 3113754," registered July 11, 2016.
135 Email from Steven Glicker on World Wide Web Consortium chat forum, dated April 5, 2006.
136 Scahill and Greenwald, op. cit.
137 "Small Footprint Operations 2/13," Document posted on The Intercept, October 15, 2015.
138 Pat Sullivan, "Gold Coast Conference Small Businesses & PEO C4I presentation," Navy's Small Business Innovation Research program, August 23, 2011.
139 Nick Wakeman, "Six3 makes Intel Deal," Washington Tecnology, April 25, 2012. Doug Cameron, "CACI Buys Intelligence Specialist," Wall Street Journal, October 9, 2013.
140 Henneberger v. Ticom Geomatics, op. cit.
141 Ibid.
142 Ibid.
143 "Airstrikes Launched Amid Intelligence Gaps," Ocala Star-Banner, October 1, 2014.
144 Scott Shane, "Drone Strikes Reveal Uncomfortable Truth: U.S. is Often Unsure Who Will Die," New York Times, April 23, 2015.
145 Kate Clark, "The Takhar Attack: Targeted Killings and the Parallel Words of U.S. Intelligence and Afghanistan," Afghan Analyst Network, May 10, 2011.
146 Steve Ressler, "Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research," Homeland Security Affairs journal, July 2006.
147 Alexander Dryer, "How the NSA Does 'Social Network Analysis,'" Slate, May 15, 2006.
148 Vladis Krebs, "Connecting the Dots Tracking Two Identified Terrorists," Orgnet 2007.
149 Michael Flynn, Rich Juergens, and Thomas Cantrell, "Employing ISF SOF Best Practices," Joint Forces Quarterly, 3rd Quarter 2008.
150 Charlie Savage, "Government Releases Once-Secret Report on Post-9/11 Surveillance." New York Times, April 24, 2015.
151 Barton Gellman, "Is the FBI up to the Job 10 Years After 9/11?" Time, May 12, 2011.
152 Matthew Erlacher, "Fighting Dark Networks: Using Social Network Analysis to Implement the Special Operations Targeting Process for Direct and Indirect Approaches," Naval Postgraduate School, March 2013.
153 Cited in Kate Clark, "The Takhar Attack: Targeted Killing and the parallel worlds of US intelligence and Afghanistan," Afghanistan Analysts Network, May 5, 2011.
154 "Afghan Raids Common, But What if the Target is Wrong?" Morning Edition, May 12, 2011.
155 Clarke, op. cit.
Stephen Grey, "The New Spymasters: Inside Espionage from the Cold War to Global Terror," St. Martin's Press, July 2015.
156 Cockburn, op. cit.
157 Ahmad Zaidan. "Al Jazeera's A. Zaidan: I am a journalist not terrorist," Al Jazeera, May 15, 2015.
158 Ibid.
159 Interview with Ahmad Zaidan, PBS Frontline.
160 Books by Peter Bergen, Peterbergen.com, undated. Accessed June 13, 2017.
161 Cora Currier, Glenn Greenwald and Andrew Fishman, "U.S. Government Designated Prominent Al Jazeera Journalist As "Member Of Al Qaeda," May 8, 2015.
"SKYNET: Courier Detection via Machine Learning," The Intercept, May 8, 2016.
162 Christain Grothoff and J.M. Porup. "The NSA's SKYNET program may be killing thousands of innocent people," Ars Technica, February 16, 2016.
163 Zaidan, op. cit.
164 "Take me off Trump's Kill List, Journalists Urge US Courts," Reprieve press release, March 31, 2017.
165 Sebastian Schaffert, "Semantic Wikis," IEEE Software, July/August 2008.
166 Arto, "How RDF Databases Differ from other NoSQL Solutions," April 22, 2010.
167 Kristina Toutanova and Christopher D. Manning, "Enriching the Knowledge Sources Used in a Maximum Entropy Part-of-Speech Tagger," 2000 Joint SIGDAT Conference on Empirical Methods in Natural Language Processing and Very Large Corpora, October 7, 2000

168 "BLADE Semantic Wiki factsheet," Modus Operandi, undated. Accessed June 13, 2017.
169 Alex Woodie, "How Analytics is Driving Military Intelligence," Datanami, February 3, 2014
170 "Modus Operandi Awarded US Office of Naval Research Contract to Expand Intelligence Analysis Wiki," Modus Operandi press release, February 21, 2012
"U.S. Navy Selects Modus Operandi for Intelligence Analysis Counterinsurgency Targeting System," Modus Operandi press release, May 14, 2012.
171 "Modus Operandi Awarded $1 Million U.S. Army Contract for Enemy and Criminal Behavioral Recognition System," Modus Operandi press release, December 12, 2012.
"U.S. Navy Selects Mods Operandi Develop Pattern Life Analysis Software Help Predict Adversarial Behavior Intent," Modus Operandi press release, February 23, 2016.
172 Ibid.
173 Maryann Lawlor, "Googlizing Intelligence," Signal, June 2010.
174 Shane Harris, "Palantir Technologies spots patterns to solve crimes and track terrorists," Wired, July 31, 2012.
175 Ashlee Vance and Brad Stone, "Palantir, the War on Terror's Secret Weapon," Bloomberg, November 22, 2011.
176 Matt Burns, "Leaked Palantir Doc Reveals Uses, Specific Functions and Key Clients," Techcrunch, January 11, 2015.
177 William Alden, "Inside Palantir: Silicon Valley's Most Secretive Company," BuzzFeed, May 6, 2016.
178 Kate Wilson, "Analyzing the Data Behind Skin and Bone," The International Consortium of Investigative Journalism, July 19, 2012.
179 Jen Judson, "Judge Rules in Favor of Palantir in Lawsuit Against US Army," Defense News, October 31, 2016.
180 "Halogen Unconventional Intelligence for the 21st Century factsheet," Lockheed Martin, undated. Accessed June 13, 2017.
"LM Wisdom factsheet," Lockheed Martin, undated. Accessed June 13, 2017.
181 "Introducing Dragon Dome factsheet," Lockheed Martin, undated. Accessed June 13, 2017.
"GeoLAMP Geospatial Large Area Multi-Sensor Processor factsheet," Lockheed Martin, undated. Accessed June 13, 2017.
182 Tom Temin, "Have you Visited the Deep, Dark Web Recently?" Federal News Radio, July 3, 2015.
183 Susan Berfield, "How Walmart Keeps on Eye on its Massive Workforce," Bloomberg, November 24, 2015.
184 James Kitfield, "Airpower Comes of Age," Air Force magazine, September 2015.
185 Air Force DCGS factsheet, op. cit.
186 Robert Dimichele "New DCGS-A Capabilities Improve Intelligence Gathering Processes," U.S. Army public affairs, July 13, 2016.
187 "Air Force Doctrine Document 2-0," January 6, 2012.
188 Air Force DCGS factsheet, op. cit.
189 Air Force DCGS factsheet, op. cit.
190 Greg Slabodkin, "Distributed Common Ground System Comes Under Fire," Defense Systems, October 1, 2012.
191 Oriana Pawlyk, "Leaders monitor burnout among intel analysts," Air Force Times, November 22, 2014.
192 Roger Mola, "The Intel Web," Air & Space September 2016.
193 "1N1 to be Questions," Air Force Enlisted chat forum, December 7, 2015.
194 Canaday, op. cit.
195 "Case Study: Air Force Distributed Common Ground System," Institute for Defense Analyses, May 20, 2015.
196 "Subject: Air Force Distributed Common Ground System (AF-DCGS), System Release 3.0 Operational Utility Evaluation," Memorandum from Operational Test & Evaluation Directorate (DOT&E), Department of Defense, July 20 2016.
197 "Distributed Common Ground System Army 2012 factsheet," Available on the website of globalsecurity.org
198 Jason Brown, "Strategy for Intelligence, Surveillance, and Reconnaissance," Forces Quarterly, 1st Quarter 2014.
199 Whittle, op. cit.
200 Brown, op. cit.
201 Jason Brown and David Vernal, "Time-Dominant Fusion in a Complex World," Trajectory magazine, November 11, 2014.
202 Biography of Colonel Jason M. Brown, Air Force website, posted May 2016.
203 Mola, op. cit.
204 Mola, op. cit.
205 Al Rockett, "What is ISR? Find Out What the Two Most Secretive Wings at Langley AFB do," Daily Press, July 5, 2017.
206 Biography of Colonel Michael Stevenson, Air Force website, March 2015.
207 Rockett, op. cit. Cahn, op. cit.
208 Jason Green, "Integrating Mission Type Orders Into Operational Level Intelligence Collection," National Defense University, May 27, 2011.
209 "Q&A: Major General Robert P. "Bob" Otto," Tactical ISR Technology, November 27, 2012.
210 Mola, op. cit.
211 "Subject: Air Force Distributed Common Ground System (AF-DCGS)," Memorandum from Operational Test & Evaluation Directorate (DOT&E), Department of DefenseAugust 12, 2010.
212 "Subject: Air Force Distributed Common Ground System (AF-DCGS)," Memorandum from Operational Test & Evaluation Directorate (DOT&E), Department of Defense, August 28, 2014.
213 Ibid.
214 DOT&E evaluation of AF-DCGS, 2016, op. cit.
215 DOT&E evaluation of AF-DCGS, 2016, op. cit.
216 Rowan Scarborough "Army Tells Officers to Fight Duncan Hunter Over Battlefield Intelligence System," Washington Times, April 2, 2014.
217 Robert Draper, "Boondoggle Goes Boom," New Republic, June 18, 2013.
218 Scarborough, op. cit.
219 Ellen Mitchell, "How Silicon Valley's Palatir Wired Washington," Politico, August 14, 2016.
220 Amber Corrin, "Lawmaker alleges DCGS-A down during hospital airstrike," C4ISRNET, October 21, 2015.
221 DOT&E evaluation of DCGS-A, 2016, op. cit.
222 "Advance Cockpit Ground Control Station fact sheet," General Atomics website, undated. Accessed June 13, 2017.
"Universal Ground Control System factsheet," Lockheed Martin website, undated. Accessed June 13, 2017.
"Ground Control Station for Northrop Grumman's Fire Scout Successfully Completes U.S. Navy Acceptance Test," Northrop Grumman press release, June 18, 2002.
223 "Air Force Military Occupational Specialty List," undated. Accessed June 13, 2017.
224 David Deptula, "The Way Ahead: Remotely Piloted Aircraft in the United States Air Force," presentation to the Air Force Scientific Advisory Board, January 2010.
225 Clausen, op.cit.
226 Hennigan, op. cit.

227 "Battlefield Airborne Communications Node factsheet," Northrop Grumman website, undated. Accessed June 13, 2017.
228 Rob Blackhurst, "The Air Force Men who Fly Drones in Afghanistan by Remote Control," Daily Telegraph, September 24, 2012.
229 Brian Everstine, "Inside the Air Force's drone operations," Air Force Times, June 22, 2015.
230 "RQ-4 Global Hawk factsheet," Air Force website, October 27, 2014.
Kenji Thuloweit, "AF Plant 42 keeps the U-2 Dragon Lady flying at 60," 412th Test Wing Public Affairs, August 27, 2015
231 Alan Axelrod, "Mercenaries: A Guide to Private Armies and Private Military Companies," 2014.
232 Ibid.
233 Whitlock, op. cit.
234 Brian Everstine, "AWACS for the 21st Century," Air Force magazine, January 2016.
235 "U-2 High Altitude Reconnaissance Aircraft factsheet," Airforce Technology, undated. Accessed June 13, 2017.
236 Abigail Fielding-Smith and Crofton Black, "Reaping the rewards: How private sector is cashing in on Pentagon's 'insatiable demand' for drone war intelligence," The Bureau of Investigative Journalism, July 30 2015.
237 Job advertisement for Geolocation Operator, Leidos. Accessed June 13, 2017.
Job advertisement for Geolocation Operator, BAE Systems. Accessed June 13, 2017.
238 Job advertisement for Ground Moving Target Indicator Analyst, Altamira. Accessed June 13, 2017.
239 Air Force DCGS factsheet, op. cit.
240 David Hubler, "Air Force Takes Aim at DART Intel System Expansion," Defense Systems, February 16, 2012.
241 "Air Force Intelligence Surveillance And Reconnaissance Agency Instruction 14-153 Volume 3," February 5, 2014.
242 "One for All: AAI Textron's UAV Control System," Defense Industry Daily, January 15, 2013.
243 Fielding-Smith and Black, op. cit.
244 "Tactical Pocket Guide for Organic/Non Organic Group 3/4/5 UAS, Joint Unmanned Aircraft System Center of Excellence," Air Force, February 2010.
245 Ibid.
246 Ibid.
247 Anna Mulrine, "Warheads on Foreheads," Air Force magazine, October 2008.
248 Briefing by Colonel James Bitzes at New America Foundation, February 24, 2011.
249 W.J. Hennigan, "Air Force to Allow Non-Officers to Fly Drones for the First Time," Los Angeles Times, December 17, 2015.
250 "Unmanned Aerial Systems: Actions Needed to Improve DOD Pilot Training," Government Accountability Office, May 2015.
251 Sandra Erwin, "A Booming New Business? Drone Pilot Training," Bloomberg, December 21, 2015.
252 Dan Gettinger, "The Surrogate Predator Program," Center for the Study of the Drone, January 25, 2016.
253 Interview with Dr. Wayne Chappelle, July 2015.
254 Neil Genzlinger, "'Drone' Documentary Examines a New Weapon," New York Times, November 19, 2015.
Jeannette Catsoulis, "'National Bird' Follows Whistle Blowers in America's Drone War," New York Times, November 10, 2016.
George Zornick, "New Film Highlights the Human Cost of Drone Warefare," The Nation, October 24, 2013.
255 Linebaugh, op. cit.
256 Zornick, op. cit.
257 "From Flightline to Intel Shortfall," Post by RaulNorry on Reddit chat forum, 2016.
258 Whittle, op. cit.
259 Dino Brugioni, "Eyes in the Sky: Eisenhower, the CIA and Cold War Aerial Espionage," Naval Institute Press, March 2010
260 Whittle, op. cit.
261 Aram Roston, "The Colonel and his Labyrinth," Vocativ October 30, 2013.
262 Ibid.
263 "Sierra Nevada Corporation Achieves Milestone for USAF's Advanced Wide-Area Airborne Persistent Surveillance System – Gorgon Stare Increment 2," Sierra Nevada Corporation press release, July 1, 2014.
264 Whittle, op. cit.
265 Winslow Wheeler, "The Problems with the 'Gorgon Stare' Surveillance System," Counter Punch, January 25, 2011.
266 "Division 312 Electronics, Sensors, and Networks Research factsheet," Office of Naval Research website, undated. Accessed June 13, 2017.
267 "About PEO IEW&S," Army website, undated. Accessed June 13, 2017.
268 "The Ground Based Common Sensor Program," Office of the Inspector General, Department of Defense July 26, 1999.
269 Ibid.
270 Elizabeth Book, "US: Prophet Rushed to the Field for Intelligence Collection," National Defense magazine, April 1, 2002.
271 Shane Harris, @War, "The Rise of the Military-Internet Complex," Houghton Mifflin Harcourt, 2014
272 Moises Gutierrez, "Learning Under Pressure: PM ODI Builds on Experiences in Iraq and Afghanistan to Adapt and Improve on Numerous Fronts," U.S. Army PEO IEW&S News, April 16, 2012.
273 U.S. military cable, Wikileaks Afghan war diaries, September 4, 2009.
274 "Backgrounders: Best Practices in Counterinsurgency – Operation Seventh Veil," Institute for the Study of War, April 1, 2010.
275 Based on a review of U.S. military cables in the Wikileaks Afghan war diaries. See.
276 Ibid.
277 Ibid.
278 U.S. military cable, Wikileaks Afghan war diaries, October 26, 2009.
279 Kris Osborn, "After Iraq Success, Military Takes Tactics to Afghanistan," Defense News, January 21, 2008.
280 Spencer Ackerman, "High Tech Army Team Turns from Killers to Airborne Spies," Wired, August 16, 2010.
281 Ibid.
282 "Kevin Ducky Hoffmann Joins Intuitive As The Director Of Air Force Programs," Intuitive Research and Technology Corporation press release, October 2010. Accessed June 13, 2017.
283 Ed Topps LinkedIn profile.
284 James Drew, "Sierra Nevada-Intuitive Team Confirmed as Fourth JSTARS bidder," Flight Global, September 1, 2015.
285 Barack Obama speech, "Drone policy and counter terrorism," New York Times May 23, 2013.
286 John Arquilla and David Ronfeldt, "In Athena's Camp: Preparing for Conflict in the Information Age," RAND Institute, 1997

287 George Crawford, "Manhunting: Counter-Network Organization for Irregular Warfare," Joint Special Operations University, September 2009.
288 Law Enforcement's Policies on Facial Recognition Technology, House Committee on Oversight and Government Reform hearing, March 22, 2017.
289 Ibraheim Mashal, "I'm a Former Marine who was on the No Fly List for 4 Years-I Still Don't Know Why," American Civil Liberties Union blog, July 1, 2016.
290 Cockburn, op. cit.
291 Noah Shachtman, "How Technology Almost Lost the War: In Iraq, the Critical Networks are Social – Not Electronic," Wired, November 11, 2007.
292 Robert H. Scales Jr., Testimony before House Armed Services Committee, October 21, 2003.
293 Canaday, op. cit.
294 "The Immutable Nature of War," PBS, May 4, 2004.
295 "CBP Drones are Dubious Achievers," Office of Inspector General, Homeland Security, January 6, 2016.
296 Rep. Candice Miller Questioning Witnesses on Securing the Maritime Border, House Homeland Security Committee, July 14, 2015.
297 Performance Audit of Department of Defense Intelligence, Surveillance, and Reconnaissance, House Permanent Select Committee on Intelligence, April 2012
298 Defense Science Board 2008 report, op. cit.
299 Spencer Ackerman, "U.S. Drone Strikes More Deadly to Afghan Civilians than Manned Aircraft – Adviser," The Guardian July 2, 2013.
300 Ryan Devereaux, "Manhunting in the Hindu Kush," The Intercept October 15, 2015.
301 Cloud, op. cit.
302 Vicki Divoli speaking on camera in 'Unmanned' documentary, October 2013.
303 David Rohde, "What the United States Owes Warren Weinstein," The Atlantic April 28, 2015.
304 Winslow Wheeler, "Revolutionary…or Routine?," Time magazine, March 2, 2012.
305 "Intelligence, Surveillance and Reconnaissance (ISR) Portfolio Valuation tool factsheet," Booz Allen website, undated.
306 Jon Schwarz, "Drones, IBM, and the Big Data of Death," The Intercept, October 23, 2015.
307 "Evolutionary Acquisition," MITRE Systems Engineering Guide, undated, Accessed June 13, 2017.
308 "Test & Evaluation Management Guide 6th Edition," Defense Acquisition University Press, December 2012.
309 John Keller, "General Atomics to build 24 MQ-9 Block 5 Reaper Attack Drone in $279.1 million Air Force Contract," Military & Aerospace Electronics, February 5, 2015.
310 Amy Butler, "Why Global Hawk Block 40 May be Killed," Aviation Week, February 25, 2013.
311 "F-35 Joint Strike Fighter: DOD Needs to Complete Developmental Testing Before Making Significant New Investments," Government Accountability Office, April 2017.
312 Whittle, op. cit.
313 "Operational Test and Evaluation Report on the Predator Medium Altitude Endurance Unmanned Aerial Vehicle," Operational Test & Evaluation Directorate, Department of Defense, September 2001.
314 Ibid.
315 "Operational Test & Evaluation Report on the MQ-9 Reaper Armed Unmanned Aircraft System," Operational Test & Evaluation Directorate, Department of Defense, March 2009.
316 Global Hawk factsheet, op. cit.
317 "Operational Test & Evaluation Report on the RQ-4B Global Hawk Block 30," Operational Test & Evaluation Directorate, Department of Defense, May 2011.
318 Cockburn, op. cit.
319 Cockburn, op. cit.
320 Ellen Nakashima & Craig Whitlock, "With Air Force's Gorgon Drone 'We Can See Everything,'" Washington Post, January 2, 2011.
321 Cloud, op. cit.
322 Most Congressional Research Service reports can be found on the website of the Federation of American Scientists.
323 See website of the Defense Contract Audit Agency (DCAA).
324 All unclassified reports of the Government Accountability Office (GAO) can be found on their website.
325 All unclassified reports of the Department of Defense Office of Inspector General can be found on their website.
326 "U.S. Army Regulation 15–6," April 1, 2016.
"Air Force Commander-Directed Investigation Guide," April 26, 2010.
327 The American Civil Liberties Union (ACLU) has successfully forced the Obama administration to release many documents on targeted killings and posted the documents on its website.
328 Talk by Chris Aaron at the Inside Drone Warfare Symposium at the University of Nevada Law School, March 30, 2016.
329 Ibid.
330 Chris Antal speaking in a Democracy Now interview: "'I Refuse to Serve as an Empire Chaplain': U.S. Army Minister Resigns over Drone Program," June 3, 2016.
331 Stephen Snyder, "The 'Empire Chaplain': This Army Clergyman Quit Over the US Drone Program," Public Radio International, May 19, 2016.
332 "I Refuse to Serve as an Empire Chaplain," Democracy Now, op. cit.
333 Brandon Bryant speaking in a Democracy Now Interview: "Numbing & Horrible': Former Drone Operator Brandon Bryant on his Haunting First Kill," November 20, 2015.
334 Ethan Levitas, "Confessions of a Drone Warrior," GQ magazine, October 23, 2013.
335 Ibid.
336 Ed Pilkington, "Life as a Drone Operator: 'Ever Step on Ants and Never Give it Another Thought?,'" The Guardian November 19, 2015.
337 Vegas Tenold, "The Untold Casualties of the Drone War," Rolling Stone, February 18, 2016.
338 Cian Westmoreland and Stephen Lewis speaking in Democracy Now Interview, "2 Air Force Vets Speak out for First Time on Why They Want the Drone War to Stop," November 20, 2015.
339 Ibid.
340 Linebaugh, op. cit.
341 Heather Linebaugh speaking in 'National Bird' documentary, November 2016.
342 Linebaugh, op. cit.
343 Linebaugh, op. cit.
344 Lisa Ling speaking in 'National Bird' documentary, November 2016.
345 Ibid.
346 Ibid.
347 "Air Force Vets Speak Out for First Time," Democracy Now, op. cit.
348 Daniel Rothberg, "At UNLV, whistleblowers call for accountability in military drone program," Las Vegas Sun, March 30, 2016.
349 Daniel speaking in 'National Bird' documentary, November 2016.
350 Ibid.
351 Lauren McCauley, "Former Drone Pilots on to Obama: Civilian Killings Driving 'Terrorism, Instability,'" Common Dreams November 18, 2015.
352 "U.S. Army Chaplain Resigns in Opposition to use of Assassin Drones by the United States," Veterans for Peace press release, May 6, 2016.

November 18, 2015

**President Barack Obama
The White House
Washington, D.C.**

**Secretary Ashton B. Carter
Department of Defense**

**Director John O. Brennan
Central Intelligence Agency**

Dear President Obama, Secretary Carter and Director Brennan:

We are former Air Force service members. We joined the Air Force to protect American lives and to protect our Constitution. We came to the realization that the innocent civilians we were killing only fueled the feelings of hatred that ignited terrorism and groups like ISIS, while also serving as a fundamental recruitment tool similar to Guantanamo Bay. This administration and its predecessors have built a drone program that is one of the most devastating driving forces for terrorism and destabilization around the world.

We witnessed gross waste, mismanagement, abuses of power, and our country's leaders lying publicly about the effectiveness of the drone program. We cannot sit silently by and witness tragedies like the attacks in Paris, knowing the devastating effects the drone program has overseas and at home. Such silence would violate the very oaths we took to support and defend the Constitution.

Sincerely,
Brandon Bryant
Cian Westmoreland
Stephen Lewis
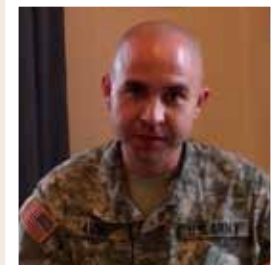Michael Haas [351]

April 12, 2016

**MEMORANDUM FOR
Commander-in-Chief, The White House,
1600 Pennsylvania Avenue, NW,
Washington, DC 20500**

THRU U.S. Army Resources Command, ATTN; AHRC-OPL-P, 1600 Spearhead Division Avenue, Ft. Knox, KY 40122

SUBJECT: Resignation in Protest

Dear Mr. President:

I hereby resign my commission as an Officer in the United States Army.

I resign because I refuse to support U.S. armed drone policy. The Executive Branch continues to claim the right to kill anyone, anywhere on earth, at any time, for secret reasons, based on secret evidence, in a secret process, undertaken by unidentified officials. I refuse to support this policy of unaccountable killing.

I resign because I refuse to support U.S. policy of preventive war, permanent military supremacy and global power projection. The Executive branch continues to claim extra-constitutional authority and impunity from international law. I refuse to support this policy of imperial overstretch.

I resign because I refuse to serve as an empire chaplain. I cannot reconcile these policies with my sworn duty to protect and defend America and our constitutional democracy or my covenantal commitment to the core principles of my religion faith. These principles include: justice, equity and compassion in human relations, a free and responsible search for truth; and the inherent worth and dignity of every person.

Respectfully submitted,
Christopher John Antal [352]

AAI Textron

General Dynamics

Northrop Grumman

Advanced Concepts Enterprises

Harris

Palantir

Hawker Beechcraft

R-4

AirScan

IBM

RadiantBlue

Altamira

Inmarsat

Raytheon

Aviation Unmanned

Intelsat

SAIC

Avwatch

Intrepid Solutions

Sentient Vision Systems

BAE Systems

L-3

SES

Boeing

Leidos

Sierra Nevada

Booz Allen Hamilton

Lockheed Martin

Spectrum

CAE

MacAulay-Brown

Ticom Geomatics

ESRI

ManTech

Transvoyant

Eutelsat

Merlin Ramco

Worldwide Language Resources

FLIR Systems

Mitre corporation

General Atomics

Modus Operandi

Zel Technologies